

Robocall Mitigation and Compliance Program of Digital Telecom & Technology Inc

1.0 Executive Summary & Commitment

Digital Telecom & Technology Inc is dedicated to the fight against illegal robocalls and caller ID spoofing. This Robocall Mitigation Plan outlines the comprehensive measures we have deployed across our network and operations to detect, prevent, and stop such unlawful traffic. Our program is designed to meet and exceed the requirements set forth by the Federal Communications Commission (FCC), including the TRACED Act and relevant sections of 47 C.F.R. § 64.6300 et seq. We are committed to continuous improvement, regularly reviewing and updating this plan to adapt to new threats and evolving regulatory standards.

2.0 Foundational Compliance & Objectives

This plan is built on several key objectives:

- **Strict Adherence to Regulations:** Full compliance with all FCC orders, including STIR/SHAKEN mandates and traceback requirements.
- **Proactive Threat Mitigation:** Using a layered approach of technology and vetting to identify and block illegal robocalls before they reach consumers.
- **Consumer Protection:** Safeguarding the public from unwanted, spoofed, and fraudulent calls.
- **Industry Collaboration:** Active cooperation with law enforcement, regulators like the FCC and FTC, and industry bodies like the USTelecom Industry Traceback Group (ITG).

3.0 STIR/SHAKEN Implementation

Digital Telecom & Technology Inc has successfully implemented STIR/SHAKEN protocols to authenticate caller ID information for all Internet Protocol (IP)-based calls, in accordance with 47 CFR § 64.6302. For calls traversing non-IP network segments, we have deployed alternative mitigation measures as permitted under 47 CFR § 64.6305, ensuring a consistent standard of scrutiny for all traffic on our network.

4.0 Subscriber and Partner Vetting (KYC)

We employ a rigorous "Know Your Customer" (KYC) framework managed by a dedicated compliance team. Before onboarding any new customer or provider, we conduct thorough due diligence, which includes:

- **Verification of Business Identity:** Reviewing the applicant's website, business purpose, and physical address for legitimacy.
- **Regulatory Cross-Check:** Screening against public enforcement actions and warning letters issued by the FCC and FTC regarding robocalling or spoofing activities.
- **Industry Reputation:** Consulting with industry contacts and reviewing historical traceback request data associated with the applicant.
- **FCC Database Verification:** Ensuring that all provider customers are properly registered and remain in good standing within the FCC's Robocall Mitigation Database.
- **Enhanced Scrutiny for High-Risk Entities:** Applying more stringent review processes for applicants with high-volume calling operations, such as call centers, or those based overseas.

5.0 Network-Based Mitigation Technologies

To actively combat illegal robocalls in real-time, we utilize a suite of network tools designed to analyze traffic patterns and filter calls:

- **Traffic Pattern Analysis:** Our systems continuously monitor network traffic for anomalies indicative of robocalling, such as abnormally high call volumes, low average call duration, and unusual Answer Seizure Ratios (ASR). This data helps us identify and flag suspicious activity for further investigation.
- **Do-Not-Originate (DNO) List Blocking:** We proactively block calls from phone numbers listed on DNO registries, including those provided by USTelecom, SOMOS, and Neustar. This includes calls from numbers that are invalid, unallocated, unused, or numbers that our own customers have requested be placed on a DNO list.
- **Call Authentication Challenges:** For traffic routed through specific pathways, we deploy interactive voice response challenges (e.g., requiring the caller to input random digits) to differentiate between human callers and automated dialing systems.
- **Automated Number Identification (ANI) Management:** We utilize ANI management to identify and block originating numbers that are repeatedly used in attempts to send suspected unlawful traffic onto our network.

- **Whitelist Management for Essential Calls:** To prevent the blocking of important communications, we maintain a whitelist for verified legitimate callers. This includes, for example, known emergency services numbers (e.g., law enforcement), government alert systems, and critical calls from verified enterprises where call patterns are well-understood and lawful.

6.0 Investigation, Traceback, and Enforcement

Digital Telecom & Technology Inc maintains a clear and rapid process for responding to suspicious activity and official traceback requests.

- **Single Point of Contact:** We have designated a primary point of contact to handle all traceback inquiries from the FCC, law enforcement, and the ITG, ensuring efficient communication.
- **24-Hour Response Commitment:** We are fully committed to responding to all official traceback requests within 24 hours, providing all necessary information to identify the source of illegal robocalls.
- **Escalation and Enforcement:** Upon confirmation of illegal robocalling activity, we take immediate action. This can include:
 1. **Suspension of Service:** Temporarily halting service for the offending party while an investigation is conducted.
 2. **Permanent Blocking:** Permanently blocking the identified illegal traffic.
 3. **Contract Termination:** Exercising our contractual rights to terminate our agreement with any customer found to be in violation of the Telephone Consumer Protection Act (TCPA) or other relevant laws.
 4. **Upstream Provider Notification:** As a gateway provider, we also work with our immediate customers to ensure they investigate and stop illegal robocalls originating from their own downstream customers.

7.0 Industry Collaboration & Data Sharing

We believe that collaboration is essential to winning the fight against robocalls. Digital Telecom & Technology Inc actively participates in industry-led initiatives, including:

- **USTelecom Industry Traceback Group (ITG):** As a participating member, we support and contribute to the ITG's efforts to trace and identify the sources of illegal robocalls.

- **Information Sharing:** We partner with organizations like YouMail to receive near real-time feeds of telephone numbers associated with active scams. This intelligence is then used to update our blocking measures. We also maintain direct lines of communication with agencies like the Internal Revenue Service (IRS) to address specific scam campaigns.

8.0 Certification

Digital Telecom & Technology Inc hereby certifies the following:

1. This Robocall Mitigation Plan is accurate and complete.
2. We are in full compliance with the requirements of 47 CFR § 64.6305.
3. We have no prior or pending FCC or law enforcement actions against us related to the origination of illegal robocalls.
4. We will maintain our registration and submit all required data to the FCC Robocall Mitigation Database.

This plan reflects Digital Telecom & Technology Inc's unwavering commitment to maintaining the integrity of the public telephone network and protecting consumers from the scourge of illegal robocalls.