

## TACIT SOLUTIONS LLC

### ROBOCALL MITIGATION PLAN

#### I. Background

The Federal Communications Commission ("FCC" or "Commission") has adopted rules requiring voice service providers, like TACIT SOLUTIONS LLC ("TACIT"), to, among other things, file certifications and robocall mitigation plans in the FCC's Robocall Mitigation Database ("RMD"). 47 CFR § 64.6305; see also Call Authentication Trust Anchor, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18 (Mar. 17, 2023) ("Sixth Caller ID Authentication Report and Order").

The FCC requires that all voice service providers certify in the Commission's RMD whether they have implemented the STIR/SHAKEN authentication framework, and that all of the calls that they originate, carry, or process are subject to a robocall mitigation program consistent with the Commission's rules. The provider's mitigation plan shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. 47 C.F.R. § 64.6305(a)(2); *id.* at § 64.6305(b)(2)-(c)(2).

The Commission's rules and the TRACED Act define robocall violations by reference to violations of Sections 227(b) and 227(e) of the Communications Act of 1934. TACIT's robocall mitigation efforts focus on preventing calls that violate the Telephone Consumer Protection Act ("TCPA") and the Truth in Caller ID Act, including calls made using an automatic telephone dialing system or artificial or prerecorded voice, and calls that transmit misleading or inaccurate caller identification information with intent to defraud, cause harm, or wrongfully obtain anything of value.

The Commission has stated that a robocall mitigation program is sufficient if it includes detailed practices that can reasonably be expected to significantly reduce the origination or carriage of illegal robocalls and if the provider complies with the practices described in its plan. TACIT is

committed to implementing commercially reasonable measures to prevent illegal robocall traffic and to comply fully with FCC rules.

## **II. TACIT's Know Your Customer ("KYC") Standards**

TACIT is a voice service provider and wholesale intermediate provider, including both gateway and non-gateway services, focused on business and wholesale communications customers.

As part of its customer onboarding process, TACIT undertakes commercially reasonable measures to verify customer identity, including completion of a KYC questionnaire, execution of a written service agreement, and collection of regulatory documentation where applicable. TACIT collects and verifies, as appropriate, the following customer information:

Legal business name and entity type

State or country of incorporation

Physical business address

Primary, technical, and compliance contacts with phone numbers and email addresses

Trade and/or bank references

Federal Tax ID number

FCC Form 499 Filer ID and FRN

Robocall Mitigation Database filing status

Company website or other customer-facing presence

TACIT verifies carrier customers through the FCC Form 499 database and the FCC Robocall

Mitigation Database, conducts publicly available research regarding customer history, and reviews traceback history where applicable. New customer traffic is monitored for call patterns, ASR, ACD, caller ID usage, and other indicators of traffic hygiene concerns.

### **III. TACIT's Acceptable Use Policy**

All TACIT customers are contractually bound by TACIT's Acceptable Use Policy ("AUP"), which prohibits:

Illegal, abusive, fraudulent, deceptive, or misleading activities

Unsolicited or unlawful telemarketing and advertising

Violations of the TCPA, FTC Telemarketing Sales Rule, FCC regulations, and state and federal Do-Not-Call laws

Spoofing or misrepresentation of caller identity, including violations of the Truth in Caller ID Act

TACIT reserves the right to suspend or terminate services for violations of its AUP.

### **IV. Telephone Number Authorization, STIR/SHAKEN & Attestation Logic**

TACIT has fully implemented the STIR/SHAKEN authentication framework across its entire network in compliance with 47 C.F.R. §§ 64.6302–64.6305. TACIT signs, verifies, and transmits STIR/SHAKEN information for all applicable calls.

A/B/C Attestation Assignment

TACIT assigns attestation levels as follows:

A Attestation (Full Attestation)

TACIT has a direct authenticated relationship with the customer

The customer is fully KYC-verified

The customer is authorized to use the calling telephone numbers

Calls originate directly from TACIT-managed infrastructure

#### B Attestation (Partial Attestation)

Customer identity is verified

Caller ID ownership cannot be fully verified

Traffic is subject to enhanced monitoring

#### C Attestation (Gateway / Transit Attestation)

TACIT is acting as a gateway or transit provider

Caller ID authorization cannot be confirmed

Traffic is continuously monitored for compliance

Attestation levels may be downgraded or revoked based on traffic behavior, traceback results, or policy violations.

TACIT restricts customers to originating calls only from authorized telephone numbers and prohibits unauthorized, invalid, or spoofed caller IDs.

## V. Proactive Network Monitoring

TACIT employs internal and third-party analytics to monitor traffic for potential illegal robocall activity. Monitoring includes:

Abnormal call volumes, pacing, ASR, and ACD

NPA-NXX matching between calling and called numbers

Calls from numbers on the Somos Do-Not-Originate list

Media IP addresses linked to known illegal robocalling entities

Wireless and high-risk destination analysis

TACIT utilizes third-party tools including Somos DNO services, FraudCentral RoboGuard, and ZipDX RRAPTOR.

## **VI. Enforcement Workflow**

TACIT maintains a defined enforcement process:

### **1. Alert**

Triggered by analytics, complaints, or traceback notifications

Customer is notified and traffic reviewed

### **2. Suspend**

Temporary suspension of traffic, caller IDs, or service

Customer required to take corrective action

### **3. Terminate**

Permanent termination for confirmed or repeat violations

Notification to relevant partners when appropriate

Enforcement actions may be accelerated based on severity or regulatory risk.

### **VII. Escalation & Repeat Offender Procedures**

For repeat or serious violations, TACIT may:

Immediately block offending ANIs or traffic

Terminate customer services

Revoke or downgrade attestation privileges

Increase monitoring of associated accounts

Cooperate fully with regulatory and industry investigations

### **VIII. Commitment to Traceback Cooperation**

TACIT commits to responding within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium. TACIT will cooperate fully in investigations and take prompt corrective action when illegal robocall activity is identified.