Robocall Mitigation Plan and Certification

TELECOM CONSULTING SERVICES LLC

I. CERTIFICATION

We submit the following certification to the Federal Communications Commission:

1.1 — Scope of Program. We have implemented and continue to maintain a robocall mitigation program that satisfies each requirement of 47 C.F.R. § 64.6305. This program applies to all voice traffic originating on, terminating on, or transiting our network.

1.2 — STIR/SHAKEN Status. We do **not** rely on the small-provider exemption in § 64.6304(a), which expired on June 30, 2023. We are pursuing implementation in good faith and submit this plan as our required mitigation description.

II. CALLER ID AUTHENTICATION AND ANTI-SPOOFING CONTROLS

2.1 — Current Implementation Level.

- *Full implementation:* We have deployed STIR/SHAKEN network-wide and certify under **Option 1**.

2.2 — Interim Mitigation. Where implementation remains incomplete, the program described in this document serves as our alternative mitigation measure, actively screening traffic to prevent illegal robocalls from entering, crossing, or leaving our network.

2.3 — Number Validation and Anti-Spoofing Measures. Subscribers may present only numbers we have assigned or numbers we have authorized in writing. We rely on the following named solutions to detect, flag, and block traffic from invalid, unassigned, unauthenticated, or spoofed numbers:

- **Aureon Caller ID Authentication (CIDA) with Outbound Shield**

III. CUSTOMER VERIFICATION AND DUE DILIGENCE

3.1 — Onboarding Checks. We verify the identity of every new residential, retail, and wholesale subscriber and collect a valid physical service address before service begins.

3.2 — Heightened Review for Elevated-Risk Accounts. Outbound call centers, high-volume originators, resellers, and similar accounts receive enhanced scrutiny at application, including

business validation, and remain subject to continuous real-time monitoring for unusual calling behavior.

3.3 — Upstream Provider Verification. Consistent with **47 C.F.R. § 64.1200(n)(5)**, we confirm each upstream provider's standing before exchanging traffic by:

1. Checking that the provider holds an active, non-delisted entry in the FCC Robocall Mitigation Database;
2. Obtaining and validating basic business details (legal name, address, contact information, and OCN where applicable);
3. Retaining records of each verification.

IV. TRAFFIC MONITORING AND ENFORCEMENT

4.1 — Continuous Analysis. Our automated systems examine inbound and outbound traffic in real time for indicators of illegal robocalling, including sudden volume surges, unusually brief call durations, elevated block or answer-seizure ratios, and patterns reflected in consumer complaint data.

4.2 — Response to Detected Abuse. Suspicious activity triggers immediate review. Once we confirm illegal robocalling, we act without delay — suspending or terminating the responsible subscriber or carrier account, blocking traffic from non-compliant upstream providers, and notifying law enforcement or the FCC where appropriate.

V. TRACEBACK PARTICIPATION AND 24-HOUR RESPONSE

5.1 — Round-the-Clock Contact. We maintain a dedicated contact available 24 hours a day, 7 days a week, for traceback matters.

5.2 — Response Deadline. We will provide a complete response to every traceback request from the FCC, law enforcement, and the registered traceback consortium **within 24 hours of receipt**. A complete response identifies the originating subscriber or upstream provider, supplies call detail records adequate to trace the traffic, and confirms any mitigation steps taken.

5.3 — Cooperation. We will assist fully in traceback investigations, preserving evidence and furnishing authenticated call data on request.

VI. CONTRACTUAL SAFEGUARDS

Every subscriber, reseller, and carrier agreement we enter into includes enforceable terms that:

- Prohibit illegal robocalling and caller ID spoofing;
- Require prompt cooperation with traceback requests, including the 24-hour response obligation;
- Authorize immediate suspension or termination for violations;
- Provide for financial penalties or service-level remedies for repeat or willful violations.

VII. CONTINUING COMPLIANCE

We will:

- Revisit and update this plan at least yearly, and promptly after any material operational or regulatory change;
- Audit our verification, monitoring, and traceback processes internally;
- Train staff responsible for traceback handling and the 24-hour response requirement;
- Remain compliant with the TRACED Act and all applicable FCC rules.
