

Robocall Mitigation Program

Filing entity: Muhammad Noman

FRN: <FRN>

Date: February 2 2026

Primary contact: Muhammad Noman, Managing Member, Compliance Department

Email: m.faisal125420@gmail.com | Phone (24/7): +15703164531 | Address: 701 Tillery St
Austin Tx 78702

1. Company overview and call-chain role

Capital Media Marketting is a U.S.-organized limited liability company providing wholesale VoIP origination to enterprise and call-center customers in the United States. The company:

- Acts as a voice service provider with a STIR/SHAKEN obligation, functioning as a wholesale provider originating calls for customers.
- Does not act as a gateway provider for foreign-originated traffic and is not a non-gateway intermediate/transit-only provider.
- Is not a foreign voice service provider.

We certify cooperation with the Commission, law enforcement, and the Industry Traceback Group (ITG), including responses to traceback requests within 24 hours.

2. STIR/SHAKEN implementation status and plan

Status: Partial/transitioning implementation. A portion of traffic will be signed during rollout; remaining traffic will transition to full signing.

Plan and milestones:

1. Select hosted SHAKEN signing provider (or upstream delegated signing) and execute agreement — Target: Feb 28 2026.
2. Obtain STI-PA token (or delegated certificates) and integrate SIP Identity header signing on all SBCs/trunks — Start: Feb 28 2026
3. Pilot signing on a subset of customers/trunks with attestation policy below — Target: Feb 28 2026
4. Expand to 100% of outbound IP traffic and update RMD to “Complete implementation” — Target: Feb 28 2026
5. Ongoing monitoring of SHAKEN results (verification pass rates, attestation mix, failure codes) and remediation.

Compliance commitments:

- Implement and maintain the STIR/SHAKEN authentication framework consistent with 47 CFR §64.6301 and §64.6305.
- Maintain reasonable steps to avoid originating illegal robocall traffic and respond fully to all traceback requests within 24 hours.

3. Attestation policy

We assign attestation levels based on customer vetting, number ownership, and call origination context:

- A (Full):
 - Customer identity verified; enterprise is the originating entity.
 - Calling numbers are owned/controlled by the customer or assigned with documented authority.
 - Use cases and campaigns are compliant and consent-backed.
- B (Partial):
 - Customer identity verified; enterprise is the originating entity.

- Calling numbers are assigned by us or a third party with proper authorization, but we cannot verify full end-user association.
- Applied for compliant campaigns where number provenance is sufficient but not fully customer-owned.
- C (Gateway):
- Used only in limited, risk-managed scenarios where provenance cannot be fully established; subject to heightened monitoring and potential blocking.

We do not sign traffic for unmanaged third parties and never sell attestation.

4. Customer vetting (KYC/KYB)

Before enabling service, we collect and verify:

- Legal name, EIN, formation documents, responsible officer, physical business address, and contact details.
- Use cases/campaign descriptions (e.g., solar, roofing, home services).
- Caller ID assignment/ownership proof; TFN registry records for toll-free; LOA for leased/assigned numbers.
- Consent framework for telemarketing (source, method, date/time, opt-out process, DNC suppression).
- Prohibited traffic acknowledgement (see Section 6).

We perform periodic reviews, adverse media screening, and require updates on material changes.

5. Calling compliance requirements for customers

Customers must:

- Comply with TCPA, TSR, and FCC rules (47 CFR §64.1200, §64.1601) including truthful caller ID, time-of-day limits, abandonment/answering machine rules, and honoring DNC.
- Use only authorized caller IDs; no spoofing of government, emergency, or DNO numbers.
- Maintain opt-out mechanisms and suppress leads within 24 hours.
- Adhere to applicable state telemarketing laws and registration requirements.

6. Prohibited and restricted traffic

We block or refuse traffic involving:

- Impersonation of government agencies, financial institutions, healthcare, or emergency services.
- Known scam categories (student loan forgiveness scams, Medicare fraud, warranty scams, etc.).
- Numbers on Do-Not-Originate (DNO) lists, invalid/unallocated numbers, or ANI manipulation.
- High-risk short-duration/ping traffic indicative of illegal robocalls.

7. Monitoring, analytics, and blocking

We monitor in real time:

- Short-duration ratios, ASR/ACD anomalies, call velocity spikes, termination complaints, SHAKEN verification failures, and attestation distribution.
- Complaints and tracebacks via ITG and downstream partners.

Actions:

1. Immediate investigation upon anomaly or traceback notice.
2. Customer notification and traffic quarantine; apply enhanced analytics and rate limits.
3. Progressive enforcement: warning → suspension → termination; report egregious activity and cooperate with authorities.
4. Document root cause and mitigation; update filters and rules.

8. Traceback cooperation

Primary compliance/traceback contact:

- Name: Muhammad Noman
- Email: m.faisal125420@gmail.com
- Phone (24/7): +15703164531

We commit to responding to traceback inquiries within 24 hours, providing call detail records, origination customer identity, and consent evidence where applicable.

9. Record retention

We retain for at least 24 months:

- KYC/KYB documents, consent evidence, LOAs, caller ID assignments.
- Call metadata (timestamps, A/B numbers, trunk, attestation, SHAKEN results).
- Traceback correspondence and remediation records.

10. Numbering and caller ID management

- Validate caller IDs against authoritative databases (LERG/NPAC/TFN Registry) and DNO lists.
- Prohibit CLI rotation intended to evade blocking or attribution.
- Maintain assignment logs linking numbers to customers and campaigns.

11. Foreign traffic policy

We do not accept foreign-originated traffic for injection into the U.S. PSTN as a gateway provider. If such service is added in the future, we will update our RMD filing and implement additional gateway controls.

12. Employee training and governance

Compliance staff receive periodic training on SHAKEN, traceback procedures, TCPA/TSR, and internal policies. Program ownership: Compliance Department; escalation to Managing Member.

13. Program updates

We review this program at least annually and upon material changes (new services, regulatory updates, or gateway role). Revised versions are published to customers and filed with the FCC RMD as required.

Muhammad Noman

Muhammad Noman, Managing Member

Capital Media Marketing

Date: Feb 2 2026