

ROBOCALL MITIGATION PROGRAM DESCRIPTION

1. OBJECTIVE, SCOPE & REGULATORY CONTEXT

ShrikeTech Consulting Limited ("ShrikeTech") establishes this formal Robocall Mitigation Program Description to meet regulatory obligations mandated by the Federal Communications Commission (FCC) under 47 CFR § 64.6305. ShrikeTech operates exclusively as a foreign voice service provider based in Nigeria, delivering wholesale Session Initiation Protocol (SIP) trunking and corporate Voice over IP (VoIP) communication capabilities to verified business enterprises operating within West Africa.

Because ShrikeTech's operations terminate traffic originating outside the North American Numbering Plan (NANP)—specifically deploying valid, reachable local Nigerian telephone identities mapped under the +234 country code—the company does not possess direct access to the United States STIR/SHAKEN token-signing certificate hierarchy. Accordingly, ShrikeTech registers within the Robocall Mitigation Database (RMD) under **Option 3 (No STIR/SHAKEN Implementation)**, satisfying federal standards via the comprehensive technical, administrative, and behavioral traffic policing controls detailed herein.

2. KNOW YOUR CUSTOMER (KYC) IDENTITY & SOURCE VERIFICATION

ShrikeTech mandates a rigorous, non-negotiable identity screening framework for all enterprise accounts prior to configuring network trunks, assigning routes, or authorizing external voice pathways. This policy ensures services are provisioned only to verifiable commercial operators:

- **Corporate Registry Verification:** Every business entity must supply current incorporation credentials issued by the Nigerian Corporate Affairs Commission (CAC). ShrikeTech compliance personnel verify active status and corporate alignment directly via the official public CAC database.
- **Fiscal Integrity Scrutiny:** Applicants must submit their official Tax Identification Number (TIN) authenticated by the Federal Inland Revenue Service (FIRS) to reinforce statutory corporate trace accountability.
- **Operational Declarations:** New clients must declare their intended use-case profiles, typical outbound volume patterns, and an explicit justification for routing voice streams toward North American public switched telephone networks (PSTN).
- **Downstream Resale Restrictions:** ShrikeTech enterprise service level agreements strictly prohibit corporate accounts from wholesaling, multiplexing, or sub-allocating service channels to unverified third-party dialing networks or high-volume telemarketing agencies.

3. INFRASTRUCTURE ENGINEERING CONTROLS & CUSTOM DIALPLAN ENFORCEMENT

ShrikeTech's centralized core network switching architecture leverages an **Asterisk-based platform managed via custom FreePBX configurations**. Engineering controls are explicitly designed to maintain header validation and prevent out-of-boundary call origination before traffic transitions to international gateway transit partners (such as Voxbeam):

- **P-Asserted-Identity (PAI) and From Header Alignment:** To satisfy screening validation rules applied by intermediate carrier networks, the Asterisk core is explicitly configured at the trunk level to enforce valid, routable, and internationalized E.164 formatting on all outbound SIP INVITE messages. The system actively asserts:

```
From: <sip:+234XXXXXXXXX@your-domain-or-IP>  
P-Asserted-Identity: <sip:+234XXXXXXXXX@your-domain-or-IP>
```

- **Enforcement of Local Reachable Outbound IDs:** ShrikeTech strictly configures custom dialplan blocks to restrict customers to using authentic, verified local numbers assigned specifically to their authorized enterprise profile. Every outbound caller ID number passed into the network boundary must remain reachable and capable of handling an immediate live-answer callback from any U.S. or Canadian destination.
- **Proactive Spoofing Defenses:** Custom context parameters written into the Asterisk configurations automatically intercept inbound customer packets. Any attempt by an internal corporate trunk to spoof or transmit an unauthorized U.S. or Canadian caller identity (`+1`), a premium-rate prefix, or an unallocated directory string is dropped instantly at the ingress Session Border Controller (SBC) and softswitch layer, preventing transmission to egress pathways.

4. TRAFFIC ANALYTICS & REAL-TIME ANOMALY POLICING

ShrikeTech utilizes automated analysis tools to continuously evaluate call detail records (CDR) and channel event logging (CEL) data streams within the FreePBX environment. The softswitch evaluates systemic calling trends against known robocall behavior markers:

- **Calls Per Second (CPS) Restrictions:** Network trunks are bounded by rigid CPS ceilings aligned with authentic human B2B operational needs. Sudden spikes in concurrent call setups trigger immediate automated rate-limiting.
- **Short-Duration Monitoring:** The system computes the percentage of completed sessions lasting under six (6) seconds. High ratios of short-duration traffic flag the trunk for automated containment and manual engineering audit.
- **Answer Seizure Ratio (ASR) Tracking:** Abrupt downward deviations in standard Answer Seizure or Call Completion Rates indicate untargeted list-dialing patterns. Anomalous metrics result in automated trunk suspension pending operational verification.

5. MANDATORY 24-HOUR TRACEBACK COOPERATION COMMITMENT

ShrikeTech acknowledges its responsibility to cooperate with enforcement agencies, the FCC, and the Industry Traceback Group (ITG) to eliminate unlawful voice traffic. ShrikeTech issues an absolute operational commitment to fully cooperate with official voice traceback investigations.

Upon receiving a formal traceback inquiry concerning traffic passing through ShrikeTech routing infrastructure, a designated network operations engineer will isolate the specific upstream origin trunk, review core platform SIP session logs, and supply complete upstream attribution data **within twenty-four (24) business hours** of the initial request.

For traceback requests, investigative routing requests, or emergency compliance updates, ShrikeTech preserves a specialized corporate clearing channel monitored directly by the compliance officer:

Email: compliance@shriketech.com

6. STRICT ACCOUNT TERMINATION LIFECYCLE

ShrikeTech executes a zero-tolerance operational rule set against traffic fraud and malicious voice transmissions. If automated network behavioral monitoring or an official external traceback confirms that an enterprise client has violated terms of service to stream unauthorized robocalls:

1. **Immediate Revocation:** The corresponding Asterisk SIP trunk account profile is placed into an administrative lock status, immediately dropping all active channels.
2. **Mandatory Review:** ShrikeTech demands comprehensive traffic evidence audits from the client's executive contacts.
3. **Permanent Deactivation:** If the client fails to justify the traffic anomalies or provides fraudulent validation data, the account is permanently closed, all deposits are forfeited, and details are logged for regulatory disclosure.

Authorized Officer Signature:

/s/ Adeoye Oke

Adeoye Oke

Compliance Officer, ShrikeTech Consulting
Limited

Date of Verification:

June 22, 2026

Executed Under Penalty of Perjury
(Form RMD-3 Submission)