



ROBOCALL MITIGATION PROGRAM DESCRIPTION

FCC Robocall Mitigation Database Filing
Voice Service Provider – No STIR/SHAKEN Implementation

1. Company Identification

Legal Name: NGN CORP SAL Offshore
FCC Registration Number (FRN): 0038097374
Country of Incorporation: Lebanon

Registered Business Address:
7th Floor #B, Jdeideh 19 Center
Pierre Gemayel Avenue
Jdeideh, Maten
Lebanon

Regulatory & Traceback Contact:
Email: frn@ngncorp.com

NGN CORP SAL Offshore (“NGN CORP”) is a Lebanon-based voice carrier providing U.S. Direct Inward Dialing (DID) numbering services to established enterprise customers for legitimate inbound business communications.

2. Scope of Services and Traffic Model

NGN CORP:

- Assigns U.S. DID numbers to verified enterprise customers.
- Primarily supports inbound calling use cases.
- Routes calls to designated enterprise facilities outside the United States.
- Maintains direct contractual relationships with customers.
- Does not provide open-access retail dialing platforms.
- Does not knowingly support high-volume unsolicited outbound robocall traffic.



- Does not knowingly facilitate spoofing, scam campaigns, or fraudulent calling schemes.

NGN CORP does not operate U.S.-based PSTN gateway facilities and does not directly control U.S. domestic authentication infrastructure.

3. STIR/SHAKEN Implementation Status

NGN CORP has selected “**No STIR/SHAKEN Implementation**” (**Option 3**) in its FCC Robocall Mitigation Database certification.

NGN CORP does not originate outbound voice traffic into the U.S. PSTN using U.S. numbering resources as part of its core service model. Where interconnection with the U.S. PSTN occurs, it is through U.S.-based carrier partners responsible for authentication and compliance within their networks.

Although NGN CORP is not currently subject to direct STIR/SHAKEN implementation obligations, the company maintains a documented and enforced robocall mitigation program as outlined below.

If service offerings or traffic patterns change in the future in a manner that would trigger STIR/SHAKEN obligations, NGN CORP will update its certification and compliance posture accordingly.

4. Governance and Compliance Oversight

NGN CORP maintains internal responsibility for regulatory compliance and robocall mitigation oversight.

- A designated compliance function reviews customer onboarding.
 - Technical personnel monitor traffic behavior.
 - Management retains authority to suspend or terminate services immediately upon detection of suspicious or unlawful activity.
 - Policies are reviewed periodically to align with FCC rules and carrier best practices.
-

5. Customer Due Diligence and Onboarding Controls

NGN CORP applies risk-based due diligence prior to service activation.



5.1 Entity Verification

Before provisioning U.S. DIDs, NGN CORP collects and verifies:

- Corporate registration documentation.
- Proof of business address.
- Authorized signatory identification.
- Description of intended service use case.
- Nature of customer business activities.

Where applicable, beneficial ownership information is reviewed.

5.2 Risk Assessment

Customers are assessed for risk factors including:

- Industry type.
- Call center or automated dialing activity.
- Marketing-related traffic models.
- Prior abuse indicators.
- Geographic risk exposure.

High-risk use cases may be declined.

5.3 Contractual Safeguards

Customer agreements explicitly prohibit:

- Illegal robocalling.
- Unlawful caller ID spoofing.
- Transmission of fraudulent or scam-related traffic.
- Violations of U.S. telecommunications laws.
- Evasion of traceback or carrier investigations.

Contracts grant NGN CORP the unilateral right to:

- Suspend DIDs immediately.
 - Block traffic without prior notice.
 - Terminate agreements for regulatory violations.
 - Refuse reinstatement.
-



6. Traffic Monitoring and Network Controls

NGN CORP employs active traffic monitoring and anomaly detection measures.

Monitoring includes review of:

- Call volume irregularities.
- Short-duration call concentration.
- High answer-seizure ratios inconsistent with legitimate enterprise activity.
- Sequential or repetitive dialing patterns.
- Signaling anomalies or malformed data.
- Suspicious caller ID presentation behavior.

Traffic exceeding internal thresholds is escalated for investigation.

Where warranted, NGN CORP may:

- Temporarily suspend traffic pending review.
- Block specific DIDs.
- Restrict routing paths.
- Require customer explanation and documentation.

7. Caller ID and Numbering Integrity Controls

NGN CORP maintains safeguards to protect the integrity of U.S. numbering resources:

- DIDs are assigned only to verified customers.
- Unauthorized caller ID manipulation is prohibited.
- Suspected spoofing incidents are investigated.
- Misused numbering resources are reclaimed immediately.

NGN CORP does not knowingly permit arbitrary or unauthorized caller ID usage.

8. Complaint Handling and Escalation Process

NGN CORP maintains a documented abuse response procedure.

All complaints, blocking notices, or traceback requests received via:



frn@ngncorp.com

are:

1. Logged and tracked.
2. Reviewed by compliance and technical personnel.
3. Evaluated using call detail records (CDRs).
4. Escalated to management where necessary.

Investigations are initiated promptly and typically within 24 hours of receiving sufficient information.

Where credible evidence of illegal robocalling or spoofing is identified, NGN CORP may:

- Immediately suspend the associated numbers.
- Block related traffic.
- Terminate the customer account.
- Report findings to relevant carrier partners.

9. Traceback Cooperation

NGN CORP commits to full cooperation with:

- The Federal Communications Commission (FCC)
- The Industry Traceback Group (ITG)
- U.S. carrier partners
- Law enforcement authorities

The company:

- Maintains call detail records sufficient to identify traffic sources.
- Responds to traceback inquiries in a timely and complete manner.
- Identifies the relevant customer or upstream source.
- Implements corrective action without delay when unlawful activity is confirmed.

NGN CORP recognizes traceback cooperation as a critical industry safeguard and treats such inquiries as high priority.

10. Record Retention



NGN CORP retains:

- Call Detail Records (CDRs)
- Customer onboarding documentation
- Service agreements
- Traffic monitoring data (where maintained)

Records are retained for a commercially reasonable period sufficient to support regulatory compliance, traceback, and investigation requirements.

11. Enforcement and Zero-Tolerance Policy

NGN CORP maintains a zero-tolerance policy toward confirmed illegal robocalling activity.

Upon verification of unlawful conduct, NGN CORP may:

- Permanently terminate services.
- Refuse future provisioning.
- Share relevant findings with carrier partners.
- Implement enhanced screening for related entities.

The company prioritizes protection of U.S. numbering resources and network integrity.

12. Ongoing Review and Commitment

NGN CORP periodically reviews its robocall mitigation program to ensure continued alignment with FCC regulations and evolving industry standards.

NGN CORP SAL Offshore is committed to:

- Responsible stewardship of U.S. numbering resources.
 - Preventing unlawful robocalls.
 - Protecting upstream carrier networks.
 - Cooperating fully with regulatory and industry traceback efforts.
-



Submitted by:

NGN CORP SAL Offshore

FRN: 0038097374

Email: frn@ngncorp.com