Robocall Mitigation Database Filings

X-NETS INC.

FRN # 0036854842

04/07/2025

Contents

INFORMATION REQUIRED BY SECTION 47 CFR § 64.6305(a)

Company Legal Information:

Name: X-NETS INC

Address: 123 BERNAL AVE

City: MOSS BEACH

State: CALIFORNIA

ZIP Code: 94038

Country: USA

Telephone: (650) 451-1787

Website: https://www.x-nets.com/

Contact for Regulatory Requirements, 911, and Law Enforcement:

Name: Majdi Abdulqader PhD

Address: 123 BERNAL AVE

City: MOSS BEACH

State: CALIFORNIA

ZIP Code: 94038

Country: USA

Telephone: (925) 383 0904

E-mail Address: majdi.abdulqader@x-nets.com

X-Nets INC Certification:

X-Nets Inc. certifies that all of the calls that it originates on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(a), which shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond fully and 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.

X-Nets Networks also certifies that any prior certification has not been removed by Commission action, and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it originates are compliant with 47 CFR § 64.6301(a)(1) and (2).

Robocall Mitigation Implementation by X-Nets

To prevent illegal robocalls from originating or terminating on X-Nets network, and protect our end users, and ensure compliance with regulations (e.g., FCC in the US).

---

1. Call Authentication – Implement STIR/SHAKEN

Objective: Prevent caller ID spoofing and verify call legitimacy.

- **Action Items:**
  - Deploy STIR/SHAKEN framework for all SIP traffic on IP-based portions of the network.
  - Sign all outbound calls with appropriate attestation level (Full, Partial, Gateway).
  - Verify inbound calls using SIP Identity headers and reject or flag unverifiable calls.

---

2. Traffic Monitoring and Analytics

Objective: Identify and block robocall traffic in real time.

- **Action Items:**
  - Monitor call patterns (e.g., high volume, short-duration bursts, sequential dialing).

  - Deploy AI/ML tools to detect anomalies and suspicious behavior.
  - Set rate limits or alerts for unusual spikes from a specific account or trunk.

3. Call Blocking and Labeling Tools

Objective: Empower subscribers and automatically block known bad actors.

- **Action Items:**
  - Integrate with third-party robocall detection databases (e.g., Nomorobo, Hiya, TNS).
  - Implement call labeling (e.g., "Spam Likely") for untrusted calls.
  - Allow consumers to opt-in/opt-out of call blocking or labeling.

4. Know Your Customer (KYC) & Onboarding Controls

Objective: Prevent bad actors from obtaining VoIP access.

- **Action Items:**
  - Enforce strong KYC during customer onboarding.
  - Require validation for enterprise use cases with high call volumes.
  - Use automated reputation scoring of SIP endpoints and customers.

5. Caller ID Management and Validation

Objective: Ensure outbound caller IDs are authorized and traceable.

- **Action Items:**
  - Only allow outbound CLI from numbers verified and owned by the user.
  - Monitor for misuse of toll-free, government, or high-value numbers.

6. Incident Response Plan

Objective: Act quickly on robocall incidents and prevent recurrence.

- **Action Items:**
  - Establish a rapid takedown process for detected robocall sources.

- Create a dedicated abuse and complaints team.
- Report malicious traffic sources to traceback groups (e.g., USTelecom's ITG).

---

7. Regulatory Compliance & Reporting

Objective: Align with national and international robocall regulations.

- **Action Items:**
    - Register in the FCC Robocall Mitigation Database (if operating in the US).
    - Submit a detailed Robocall Mitigation Plan annually.
    - Stay updated with evolving rules from FCC, CRTC, Ofcom, etc.

---

8. Subscriber Education and Support

Objective: Inform and support users in identifying and reporting robocalls.

- **Action Items:**
    - Provide clear documentation and tools for call blocking.
    - Offer a way for customers to report robocalls or spoofed calls.
    - Regularly share updates and best practices.

---

9. Interconnect & Peering Policies

Objective: Ensure upstream/downstream providers share anti-robocall responsibility.

- **Action Items:**
    - Work only with trusted upstream carriers who enforce STIR/SHAKEN.
    - Terminate or quarantine traffic from carriers with repeated violations.
    - Include anti-robocall clauses in interconnect agreements.
