



Yeti Networks LLC Robocall Mitigation Program & RMD Compliance (TRACED Act / FCC Rules)

Entity: Yeti Networks LLC (the “Company”)

Last Updated: [February 10, 2026]

Provider Role(s): The Company operates as a voice service provider and may also, depending on call path, carry/process traffic received from upstream provider(s). This Robocall Mitigation Program applies to traffic the Company originates and/or carries or processes, as applicable.

1) Purpose and Commitment

Yeti Networks LLC is committed to cooperating with the FCC, law enforcement, and the industry traceback consortium to investigate and stop illegal robocalls and unlawful spoofing that originate on or traverse the Company’s network. The Company implements reasonable steps designed to prevent, detect, investigate, mitigate, and stop illegal robocall traffic.

2) STIR/SHAKEN Status

The Company has fully implemented the STIR/SHAKEN authentication framework on its network for originating traffic. Where applicable, the Company signs outbound calls consistent with its role and assigns attestation levels in accordance with its customer identity and number authorization controls.

3) 24-Hour Traceback Response Commitment

The Company commits to respond fully **within 24 hours** to traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to cooperate with these entities to investigate and stop illegal robocallers that use the Company’s service.

Traceback handling workflow (internal):

- **Intake:** Requests received via [support@getyeti.net] are logged immediately and escalated to the designated robocall compliance contact.

- **Validation:** Confirm identifiers (ANI, DNIS, timestamp, SIP Call-ID where available), and determine whether the Company is originating, intermediate, gateway, or terminating for the identified calls.
- **Records:** Retrieve call detail records (CDRs), SIP signaling logs (where available), customer account records, and number assignment/authorization documentation.
- **Response:** Provide complete findings and upstream/downstream handoff details as relevant; preserve supporting evidence.

4) FCC Enforcement Bureau Notices / Mandatory Blocking

When the Company receives an FCC Enforcement Bureau written notice identifying suspected illegal traffic, the Company will promptly investigate the identified traffic. If the Company's investigation determines it is the originating or gateway provider for the identified traffic, the Company will **block or cease accepting** the identified traffic and will continue to block or cease accepting the identified traffic, **as well as substantially similar traffic**, on an ongoing basis unless the Company determines the traffic is not illegal. If the Company determines the traffic is not illegal, the Company will provide the Enforcement Bureau (in writing) an explanation of why it reasonably concluded the traffic is not illegal and what steps it took to reach that conclusion.

5) Know Your Customer (KYC) — New and Renewing Customers

All voice service providers are required to know their end-user customers and to describe how they comply with this obligation.

The Company maintains a KYC program for **new and renewing customers** that includes risk-based identity verification, number authorization validation, and contractual controls.

KYC controls (risk-based, may include some or all depending on customer type):

1. Identity & Business Verification

- Collect legal entity name, DBA(s), physical address, email/phone contacts, and authorized signatory.
- Verify business registration and/or government ID for sole proprietors.
- Validate tax ID/EIN (where applicable) and confirm good standing where feasible.
- Screen for inconsistencies/red flags (recent entity creation, mismatched addresses, high-risk verticals, unverifiable web presence).

2. Beneficial Ownership / Responsible Party (where applicable)

- Identify an accountable individual (executive/owner) responsible for compliance and reachable for urgent remediation.
- Obtain verification supporting authority to contract for service.

3. Number Authorization / Caller ID Controls

- Require documentation demonstrating the customer's right to use each originating number (e.g., LOA, proof of assignment, underlying carrier documentation, or other verifiable evidence).
- Prevent use of unauthorized caller ID by enforcing caller ID policies (only approved numbers may be presented).

- Check proposed originating numbers against DNO/DNI sources and internal suppression lists.
- 4. **Use Case & Traffic Expectations**
 - Document intended use case(s), expected calling geographies, anticipated call volumes, and calling patterns.
 - For higher-risk use cases (e.g., outbound contact centers, lead gen, debt/insurance), require additional documentation such as sample scripts, compliance point-of-contact, and evidence of consent/opt-in processes as appropriate.
- 5. **Contractual Controls (End Users)**

Customer agreements and/or AUP terms typically include:

 - Prohibitions on illegal robocalls, spoofing, and unauthorized caller ID.
 - Requirement to comply with applicable FCC rules and laws governing calling and consent.
 - Right to suspend/block traffic immediately upon suspected abuse or regulator/traceback notification.
 - Requirement to cooperate with investigations and provide supporting documentation upon request.
- 6. **Controlled Enablement for New Accounts**
 - New accounts are provisioned with conservative limits (CPS and/or concurrent sessions), expanded only after successful verification and observed compliant behavior.
 - Enhanced monitoring during an initial probationary period and after material account changes.

6) Know Your Upstream Provider (KYUP) — Upstream Due Diligence

Providers must describe procedures in place to know upstream providers.

The Company maintains procedures to identify, document, and risk-assess its upstream voice provider(s), including maintaining accurate contact information and escalation paths.

Upstream provider(s):

1. **Trunking.io**
Email: info@trunking.io
Phone: +1 844-468-7865

KYUP controls include:

- Maintaining current upstream provider identification and contact paths for urgent mitigation and traceback support.
- Reviewing upstream technical interconnect and traffic expectations.
- Monitoring inbound traffic characteristics for anomalies and suspected illegal patterns, and escalating to the upstream provider when indicated.

- Including upstream-facing contractual expectations (where applicable) designed to mitigate illegal robocalls (e.g., cooperation, rapid response, traffic suspension rights).

7) Analytics, Monitoring, and Traffic Controls

The Company uses analytics to identify and mitigate illegal robocall traffic, including checking for invalid numbering, suspicious patterns, and unauthorized caller ID behavior. The Company's mitigation controls include:

A. Number Hygiene / Validation

- Do Not Originate (DNO) checks and internal suppression lists.
- Invalid phone number format detection; invalid/unknown NPAs; unassigned blocks (as data sources allow).
- Caller ID authorization enforcement (only approved customer numbers).

B. Behavioral Analytics / Pattern Detection

- Monitoring for high-volume bursts, short-duration calling, unusual ASR/ACD patterns, sequential dialing indicators, and geographic anomalies.
- Originating number reuse inconsistent with customer profile.
- Threshold-based alerting and manual review.

C. Rate Limiting / Segmentation

- Customer capacity limits (CPS and/or concurrent session limits), tightened for new or higher-risk accounts.
- Rapid-downshift / suspension workflows upon detection of suspected illegal patterns.

D. Third-Party Analytics Vendors (if any)

- Third-party analytics vendor(s) used: **[NONE]** or **[Vendor name(s)]**
(If you use any vendor at all, list them by name here.)

8) Investigation, Enforcement, and Remediation

The Company reserves the right to refuse, block, or suspend traffic from any party where illegal robocalling, spoofing, or unauthorized originating number use has occurred or is suspected.

Remediation actions may include:

- Blocking specific originating number(s) and/or terminating number(s)
- Blocking trunks, customer routes, or customer accounts
- Terminating the customer relationship
- Requiring additional KYC/authorization documentation before reinstatement

9) Internal Ownership and Contact for Robocall Mitigation

Designated Robocall Mitigation Contact:

Jon Sale

PO Box 910364, St. George, Utah 84791

support@getyeti.net

435-628-2500 Ext 1001

10) RMD Filing Hygiene (Ongoing)

- The Company will update its RMD filing **within 10 business days** of any change to required filing information.
- The Company will complete required annual recertification **on or before March 1** each year.