

Robocall Mitigation Program Description

Submitted by:

Nevtis Corp

1525 E Ontario Ave Suite 100

Corona, CA 92881

Purpose:

This Robocall Mitigation Program Description details the comprehensive measures Nevtis Corp has implemented to combat illegal robocalls in full compliance with the FCC's updated STIR/SHAKEN requirements.

1. STIR/SHAKEN Implementation and A-Attestation (Full)

Nevtis Corp has fully implemented the STIR/SHAKEN framework and achieved A-Attestation (Full) status as a U.S. originating service provider. We have obtained our own Service Provider Code (SPC) token from the STIR/SHAKEN Policy Administrator (STI-PA) and procured a digital certificate from the STI-CA peeringhub.io. This enables us to sign all outbound calls with our own certificate, ensuring compliance with the new FCC rules which prohibit reliance on third-party certificates while preserving accountability for attestation decisions.

Our prior model—depending on upstream authentication via Bandwidth.com—has been sunset. While Bandwidth.com remains our underlying carrier for network transit, all STIR/SHAKEN processes are now handled directly by Nevtis Corp:

- We independently determine the appropriate attestation level, in alignment with ATIS standards.
- All calls are digitally signed using our own STI-CA certificate (peeringhub.io), ensuring compliance with the Eighth Report and Order's prohibition on third-party certificate usage.

2. Traffic Filtering Mechanisms

- Real-time detection of anomalous call patterns (e.g., bursts or repetitive dialing).
- Reference to updated lists of known robocaller numbers.
- Automated blocking of calls originating from invalid, unallocated, or suspicious number ranges.
- Adaptive thresholding and rule sets to respond to evolving robocall strategies.

3. Real-Time Monitoring and Analysis

- AI-driven and behavioral analytics systems to monitor inbound and outbound call activity.
- Flagging of high-volume or irregular calling behavior.

- Automated alerts and quarantine measures for suspicious traffic pending further investigation.

4. Customer Education Initiatives

- Clear mechanisms to report suspected robocalls.
- Informational materials on caller ID spoofing and safe handling protocols.
- Continuous updates about robocall trends and defensive best practices.
- Responsive customer support to resolve robocall-related concerns.

5. Traceback Procedures

- Maintains detailed call logs.
- Assigns dedicated personnel to respond rapidly to traceback requests.
- Collaborates fully with the FCC, law enforcement, and industry traceback groups.

6. Compliance with Industry Standards

- Participation in the Industry Traceback Group (ITG) and other collaborative mitigation efforts.
- Regular policy updates in alignment with evolving FCC and industry requirements.
- Transparent engagement with other providers and authorities.

7. Regular Updates and Reporting

- Ongoing reviews and enhancements of mitigation methods in response to new threats.
- Submission of updated mitigation plans to the FCC's Robocall Mitigation Database (RMD), reflecting our direct STIR/SHAKEN implementation and A-Attestation status.
- Transparent documentation of mitigation effectiveness.

8. Customer Vetting Practices

- Mandatory capture of valid government IDs or corporate documents.
- Know Your Customer (KYC) checks to confirm legitimacy.
- Fraud-detection systems flagging questionable accounts for manual review.
- Subscription agreements enforcing zero tolerance for robocall abuse.
- Periodic reviews of account activity to detect and act on suspicious patterns.

Contact Information:

Compliance Officer: Juan Olmedo

Email: support@nevtis.com

Phone: 855-442-7107

Certification:

Nevtis Corp certifies that it has fully implemented STIR/SHAKEN with A-Attestation (Full), using its own SPC token and STI-CA-issued certificate (peeringhub.io), as required by current FCC rules. Our comprehensive robocall mitigation measures ensure regulatory compliance and network trustworthiness.

Date Submitted:

09/03/2025