



NUSO, LLC - Robocall Mitigation Plan

February 12, 2026

Contents

- Overview 2
 - NUSO's Commitments Include: 2
 - Enhanced Commitments and Certifications: 3
 - NUSO's Operational Roles: 3
- Responding to Traceback Requests:..... 4
 - Steps to mitigate illegal traffic upon notification: 5
- Robocall Prevention Measures:..... 6
 - Robocall Mitigation for Outgoing Calls: 9
 - Robocall Mitigation for Incoming Calls: 9
 - STIR/SHAKEN policy for direct NUSO customers: 10



Overview

As a Voice Service Provider managing over 100,000 lines, NUSO, LLC ("NUSO") has rigorously implemented comprehensive STIR/SHAKEN protocols alongside robust robocall mitigation measures. In strict adherence to the deadlines and requirements set forth by the Federal Communications Commission (FCC) in the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, as well as the directives outlined in the Report and Order(s), NUSO has established a proactive stance against illegal robocalls.

NUSO's Commitments Include:

- **Rapid Response:** Fully responding within 24 hours to Traceback Requests from the Industry Traceback Group (ITG), and civil and criminal law enforcement agencies, cooperating fully in efforts to investigate and eliminate illegal robocalls.
- **Illegal Traffic Mitigation:** Taking decisive actions to mitigate illegal traffic upon receiving formal notifications from the FCC or other bodies.
- **Robocall Mitigation and Full STIR/SHAKEN Implementation:** Enforcing comprehensive robocall mitigation and fully deploying STIR/SHAKEN to prevent the origination and receipt of illegal calls on our network.
- **Provider Verification:** Refusing traffic from any provider not registered in the Robocall Mitigation Database (RMD).
- **Customer Due Diligence and KYC:** Mandating that all potential customers complete a Know Your Customer (KYC) form and undergo a thorough due diligence process prior to becoming a customer. This step is crucial for assessing the legitimacy and operational integrity of new clients, ensuring that our network remains secure and compliant with regulatory standards.
- **Implementation of DNO Lists:** Utilizing Do Not Originate (DNO) lists, primarily leveraging the SOMOS and ITG lists alongside NUSO's proprietary information, to identify and block unauthorized numbers from originating and/or terminating calls.



Enhanced Commitments and Certifications:

- **Robocall Mitigation Certification:** NUSO certifies that all calls originating on our network are subjected to a robocall mitigation program that meets or exceeds the specified requirements. We affirm that our prior certifications remain unrevoked by Commission action and that we are not barred from participation in the Robocall Mitigation Database. NUSO has fully implemented STIR/SHAKEN across our network, ensuring the integrity and authenticity of calls.
- **Robocall Mitigation Plan Description:** Our robocall mitigation plan outlines the specific "reasonable steps" NUSO has undertaken to prevent the origination, transmission, or processing of illegal robocall traffic, demonstrating our commitment to upholding the highest standards of network security and customer protection.

NUSO's Operational Roles:

As a versatile entity in the telecommunications sector, NUSO functions in multiple capacities: as a direct service provider, an intermediate provider, and a U.S.-based gateway provider, catering to a wide range of customer needs, including direct retail customers beyond our wholesale operations.

Regulatory Compliance and Investigations:

NUSO is not currently, nor has it ever been, subject to any Commission, law enforcement, or regulatory agency action or investigation related to suspected unlawful robocalling or spoofing activities. This underscores our dedication to lawful and ethical operations within the telecommunications industry.

Operating Company Numbers (OCN):

Operating Company Numbers: 478J, 732J and 551G.



Responding to Traceback Requests:

NUSO actively supports the investigation of Traceback Requests and maintains a standing of good repute with the Industry Traceback Group (ITG), of which we are not only a member but also a participant in its steering committee.

For handling sensitive customer information (CPNI), NUSO adheres to strict protocols, ensuring that such information is exclusively shared through the official ITG portal. Regardless of the initial contact method—be it phone, email, or direct engagement through the ITG portal—NUSO commits to prompt investigation start. However, it's important to note that CPNI is only disclosed within the secure confines of the ITG portal.

To facilitate the traceback process, NUSO retains call records for one year. Here are the official channels through which Traceback Requests can be initiated:

- **Email:** Requests can be directed to tracebackrequest@nuso.cloud, the official email address registered with the ITG. Upon receipt, NUSO personnel will verify the request through the ITG portal before proceeding to share relevant information.
- **Direct Contact:** Paul Matte, COO, is the designated contact in the Robocall Mitigation Database, reachable at (314) 390-6260 or via email at paul.matte@nuso.cloud.
- **NUSO Website:** Users can report abuse or initiate an investigation through our support resources at <https://nuso.cloud/support/resources/acceptableuse/>
- **24x7 Support Center:** Available around the clock, our support center can be reached at (844) 438- 6876 – Option 1 for immediate assistance.



Steps to mitigate illegal traffic upon notification:

- **Step 1:** NUSO will run analysis on the reported incident(s) and determine if this traffic is indeed routing through our network.
 - If this traffic is not routing through our network, NUSO will reach back out to the reporting party for more information and to determine next steps.
- **Step 2:** If NUSO determines this traffic is indeed fraudulent, NUSO will block this traffic immediately from leaving the network. NUSO will globally block **ALL** traffic from this telephone number on any route, not just the reported fraudulent call patterns.
 - If NUSO determines this traffic is **NOT** fraudulent, NUSO will reach back out to the reporting party for more information and to determine next steps.
 - **Special Note on ITG Reports:** In cases where the report originates from the ITG, NUSO adopts a "guilty until proven innocent" stance. Such reports are presumed to be accurate, and the traffic associated with these reports is immediately blocked pending further investigation.
- **Step 3:** NUSO will contact the customer and inform them that their traffic has been blocked. The customer's traffic from this number will not be allowed back on the network until a written plan on how this traffic will be prevented is submitted, reviewed, and accepted.

Note: *In instances where NUSO receives multiple traceback requests originating from the same customer, a policy of stringent action is enforced. ALL traffic from the implicated customer may be suspended pending the submission, review, and acceptance of a comprehensive remediation plan. Should these incidents reveal systemic issues or a repeated disregard for network security protocols, NUSO reserves the right to extend the suspension into a permanent block of all traffic from the offending customer. This ultimate measure is considered on a case-by-case basis, considering multiple factors such as the severity of the violation, the frequency of incidents, and the customer's response to previous warnings and suspensions.*



Robocall Prevention Measures:

NUSO has implemented a comprehensive strategy to combat the proliferation of robocalls through our network, emphasizing our commitment to ensuring the integrity of communications and safeguarding customer trust. This strategy integrates several critical components and utilizes a combination of in-house software developed with proprietary intellectual property as well as third-party vendors to enhance detection and prevention capabilities.

Robocall Mitigation Solution: NUSO has activated an advanced robocall mitigation solution, marking a significant step in our efforts to secure the network against unwanted communications. Utilizing sophisticated analytics, NUSO assesses each call individually, applying policy-driven treatments to ensure the integrity and legitimacy of communications.

Machine Learning Technologies: NUSO leverages advanced machine learning technologies to continuously monitor network traffic, identifying irregularities and automatically blocking traffic that exhibits suspicious patterns. This is a key area where NUSO employs proprietary, in-house-developed software to analyze and act on various calling behaviors.

Our system examines multiple data points, including but not limited to:

- **Calling and Called Number Patterns:** Detecting unusual calling trends that may indicate fraudulent activity.
- **Short-Duration Calls:** Analyzing calls with abnormally short durations, which can signal potential robocall activity.
- **Repeated Attempts to Invalid Numbers:** Monitoring instances where calls repeatedly target numbers that are invalid, disconnected, or consistently return busy signals.
- **Low Answer-Seizure Ratios (ASR):** Identifying traffic with very low connectivity rates, which can indicate problematic or fraudulent calling patterns.
- **Overall Pattern Analysis:** Observing aggregated calling behaviors to identify anomalies, such as sudden spikes in call volume or unusual traffic from specific sources.

When irregularities are detected, the system takes immediate action to block suspect numbers and raises alarms for the appropriate teams to investigate further. Additionally, all analyzed data and patterns are output to a Grafana dashboard—a third-party vendor tool—providing our teams with a clear and accessible visual representation of network activity. While the dashboarding is handled externally, all underlying analysis and decision-making are powered by NUSO's in-house intellectual property.



STIR/SHAKEN Implementation: The full implementation of STIR/SHAKEN protocols underscores our commitment to call authentication and enhances the security and authenticity of telephone calls.

KYC Requirement: A stringent KYC process is mandatory for all prospective and existing clients, reinforcing our due diligence efforts to verify the legitimacy and operational compliance of customers.

Implementation of DNO Lists: Expanding our strategy to include the implementation of third-party vendor Do Not Originate (DNO) lists, most notably from SOMOS and the ITG, further enhances our ability to prevent fraudulent calls. These lists contain numbers that are not authorized to originate calls, providing an additional layer of protection against unauthorized and potentially harmful communications.

Analytics Systems and Vendors:

- **In-House Systems:** NUSO has developed robust in-house analytics using proprietary intellectual property to identify and block illegal robocall traffic. These systems leverage advanced algorithms and machine learning technologies. As described in detail under the **Machine Learning Technologies** section, our proprietary software analyzes numerous data points, such as calling patterns, call durations, and connectivity rates, to detect and mitigate suspicious activity. This comprehensive approach enables us to proactively block irregular traffic and raise alerts for further investigation, ensuring the integrity of our network.
- **Third-Party Vendors:**
 - **TransNexus:** TransNexus offers a suite of robust tools designed to combat unwanted robocalls effectively. Their solutions encompass several key features:
 - **Comprehensive Analysis of Calling Patterns:** TransNexus's platforms analyze calling behaviors to detect anomalies such as unexpected high call volumes, short call durations, and frequent call hang-ups, which are indicative of robocall activity.
 - **Intelligent Blacklisting:** The system employs intelligent blacklisting based on specific call attributes, enabling the identification and blocking of calls from known or suspected robocall sources.
 - **Detection of Invalid and High-Risk Numbers:** TransNexus solutions can identify calls originating from invalid, high-risk, or Do Not Originate (DNO) listed numbers, allowing for appropriate call handling measures such as blocking or diversion.
 - **Dynamic Traffic Analysis:** Real-time monitoring of call traffic helps detect large bursts of calls in short timeframes, a common characteristic of robocall campaigns, facilitating prompt mitigation actions.



- **STIR/SHAKEN Call Authentication:** TransNexus supports the implementation of STIR/SHAKEN protocols, which authenticate caller identities to prevent spoofing and enhance trust in caller information.

By integrating these features, TransNexus provides a comprehensive approach to identifying and mitigating unwanted robocalls, thereby enhancing the security and reliability of telecommunications networks.

- **5gVision:** 5gVision, developed by 5g Future, offers a comprehensive suite of tools designed to enhance VoIP and SMS network management, contributing to the mitigation of unwanted robocalls. Key features include:
 - **Real-Time Monitoring and Alerting:** 5gVision provides quick, web-based visual monitoring solutions that support most major softswitches. This enables operators to swiftly identify and address irregular traffic patterns indicative of robocall activity.
 - **Comprehensive Call Detail Records (CDR) Analysis:** The platform offers detailed CDR viewing with on-the-fly filtering and sorting, allowing for efficient investigation of suspicious call activities.
 - **Signaling and Media Packet Logging:** 5gVision continuously collects all signaling and media packets for any traffic volumes, facilitating in-depth analysis of call flows and detection of anomalies associated with robocalls.
 - **Flexible Alerting System:** The platform includes a flexible alerting module with notifications delivered via web, email, or SMS, ensuring timely responses to potential fraud or network issues.

By integrating these features, 5gVision assists telecom operators in effectively monitoring and managing their networks, thereby reducing the incidence of unwanted robocalls.

- **Grafana Dashboards:** Grafana is utilized to visualize and manage data from both in-house systems and third-party tools, providing a centralized platform for monitoring and analysis. By integrating real-time data streams, Grafana enables our teams to quickly identify and address irregularities, track performance metrics, and gain insights into traffic patterns. Its customizable dashboards allow for clear and actionable visualizations, enhancing our ability to maintain robust network security and operational efficiency. While Grafana handles the presentation layer, all underlying data and analysis originate from NUSO's proprietary and third-party systems, ensuring seamless integration and a comprehensive view of network activity.



Robocall Mitigation for Outgoing Calls:

- Apply analytics and tracking of abnormal calling patterns to detect high volume robocalling, spoofing, and suspicious call activity.
- Identify invalid, unallocated, and unassigned numbers to know which calls to stop, block, or tag as spam/fraud.
- Per-call dip into a Do-Not-Originate database (SOMOS, ITG, and NUSO Proprietary DNO Lists) to see if the call should be processed.
- Only allow calls to be made from authorized actors in the NUSO network.
- NUSO has put in place verification processes to ensure that NUSO customers are using phone numbers they are authorized to use.
- A connection to the NUSO network must pass authorization between the end point device (such as IP phones, Soft Phones, IP PBX's, etc.) and the NUSO authentication service.
- The number of simultaneous calls is limited to each device based on the negotiated sale. Devices are not allowed to freely process unlimited simultaneous calls.

Robocall Mitigation for Incoming Calls:

- Verify that the originator of the call into the NUSO network is in the Robocall Mitigation Database (RMDB). NUSO will not accept calls from vendors who are not in the Robocall Mitigation Database.
- Per-call fraud scoring/reputation lookup.
 - If the score returned is in the top tier of untrusted calls NUSO will block the call and not deliver to their subscriber.
 - If the score returned is in a high tier of untrusted calls NUSO will use a CNAM overlay to mark the call as potential spam/fraud before delivering to the subscriber.

Note: *The settings and actions described above can be overridden on a per telephone number basis, allowing for customized handling of calls according to specific needs or preferences of the subscriber.*

- In addition to fraud scoring and reputation lookup, NUSO incorporates STIR/SHAKEN header lookups as part of its call validation process. Calls with incorrect STIR/SHAKEN headers or missing STIR/SHAKEN information are subject to additional scrutiny. Based on this analysis, NUSO can deny delivery of calls that fail to meet the required standards of header integrity.
- NUSO will dip a global DENY list (including DNO) on all calls to determine if the inbound telephone number is allowed through the network.



STIR/SHAKEN policy for direct NUSO customers:

NUSO is committed to upholding the highest standards of call authenticity and integrity for our direct customers. This commitment is reflected in our STIR/SHAKEN policy, which is designed to authenticate call origins and ensure the legitimacy of caller information. It is important to note that this policy applies specifically to direct customers of NUSO and not to our wholesale/intermediate customers. Wholesale customers, being regulated entities, are required to implement, and manage their own STIR/SHAKEN framework and policies.

- Attestation "A":
 - Applies to calls originating from a trusted subscriber on the NUSO network who has the legitimate right to use the number in question. All numbers provided directly by NUSO to a trusted subscriber will receive an "A" attestation, signifying the highest level of trust and authorization.
 - In instances where a trusted subscriber uses numbers from other Service Providers (SVPs) that will route through the NUSO network, these calls will initially be signed with a "B" attestation. However, should the trusted subscriber furnish a written document, duly signed, asserting their authorized use of these additional numbers, NUSO will upgrade the attestation for these calls to "A".
- Attestation "B":
 - Designated for calls from a trusted subscriber on the NUSO network using a number not directly provided by NUSO or explicitly authorized by the subscriber. This attestation level indicates a moderate level of trust based on existing relationships and verifications.
- Attestation "C":
 - For direct NUSO customers, attestation level "C" is not applicable, as our relationship and thorough knowledge of our end users allow us to accurately assess and authenticate the origin of calls. Direct NUSO customers' calls are categorized with either attestation level "A" or "B". Attestation level "C" is reserved for scenarios within our wholesale operations where we do not know the originator of the call.



Paul Matte

COO

NUSO, LLC

7777 Bonhomme Ave Suite 1100

Clayton, MO 63105

314-390-6260

<https://nuso.cloud>



Recoverable Signature

X Paul Matte

Signed by: ab1c1233-0662-4a22-9be1-21d905070694