

2026 Revised Robocall Mitigation Plan

CORE Networks is a voice service provider (VSP) acting as a reseller without technical STIR/SHAKEN control of its originating calls. This is managed by Coredial (IPiFony, Bandwidth, etc.). CORE Networks is dedicated to stopping illegal calls originating in our network and to monitoring calls entering our network. The FCC requires that all VSPs certify in the Robocall Mitigation Database that they have (1) fully implemented STIR/SHAKEN across its entire network, (2) implemented STIR/SHAKEN on a portion of its network and that the remainder of the calls are subject to a Robocall Mitigation Plan (RMP), or (3) have not implemented STIR/SHAKEN but subject all calls to an RMP to ensure that the network is not originating illegal robocalls. This filing updates CORE Networks robocall mitigation efforts and procedures per FCC DA 24-73, Public Notice DA 26-72, and in compliance with 47 CFR § 64.6305.

The FCC requires that VSPs develop an RMP that:

- Lists the specific, reasonable steps the VSP has taken to avoid originating illegal robocall traffic
- States a commitment to respond fully and in a timely manner to all traceback requests from the FCC, law enforcement, and the industry traceback consortium
- To cooperate with entities investigating and stopping any illegal robocallers that use its services to originate calls

CORE Networks purchases origination, termination, and hosted-switch access from **Coredial** (“Provider”), who provides crucial elements of our RMP as part of their interconnected white-label VoIP wholesale services to CORE Networks. All voice traffic originating on our network is subject to the robocall mitigation program described below, subject to technical revisions implemented by Provider. CORE Networks does not have a parent company or any other entities controlling its operations.

Know Your Customer

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>).

International Subscribers

CORE Networks does not sell origination or termination services to subscribers outside of the United States.

Acceptable Use Policy

CORE Networks maintains an Acceptable Use Policy (“AUP”) that subscribers must accept before being permitted to use CORE Networks broadband or voice services.

Traceback Requests

CORE Networks is committed to responding in a complete and timely manner to all traceback requests from the Federal Communications Commission, law enforcement, state attorneys general, Provider, and the industry traceback consortium. Furthermore, CORE Networks is committed to cooperating with such entities to investigate and stop any illegal robocallers that use CORE Networks service to originate calls. Subscribers are required to comply with traceback requests via our AUP. Traceback requests can be sent to **support@corenets.com** for immediate processing by CORE Networks.

Telephone Number Validation

If a subscriber wishes to use a telephone number (TN) as a caller identity and that TN is not directly managed by CORE Networks or our Provider, TN validation is required, requiring the subscriber to provide a valid letter of authorization confirming they are an authorized user of that TN. Should the subscriber provide sufficient documentation to CORE Networks of authorization to use a TN, documentation will be provided to the Provider so that they can attest calls originated with these TNs.

Investigation of High-Volume Network Traffic, Suspicious Calls, and Calling Patterns

Consistent with industry standards and best practices, our Provider monitors origination voice traffic in real time to prevent the origination of illegal robocalls. The software provides detailed reporting that identifies suspected illegal robocalls and alerts the Provider if we originate any calls with an invalid, unallocated, or Do Not Originate-listed calling number, or if the calling number is in the FCC consumer complaint database or has a poor reputation. Provider will immediately ask CORE Networks to investigate any identified calls to determine whether the caller attempted to originate unlawful robocalls. If CORE Networks or Provider determines that the caller was attempting to originate unlawful robocalls, we either warn them to stop or terminate their service, in accordance with our AUP.

Examples of calling patterns monitored

- Higher than expected cost generated by calls from a subscriber
- Targeted pumping of repeated calls to a specific called number within a 15-minute period
- Fast traffic pumping of repeated calls to a specific called geographic location within a 5-minute period
- Slow traffic pumping of repeated calls to a specific called geographic location within a 60-minute period
- Theft of service traffic pumping of repeated calls to high-cost geographic location within a 60-minute period
- Recent call volumes (last 60 min) vs weekly trends
- Number of unique destination numbers in a 60-minute time frame
- Irregularities in Short Call Duration (SDC) and Average Call Duration (ACD) distribution
- Anomalies in Answer-Seizure Ratio (ASR)
- Robocalling triggers monitoring for a high-volume of outbound calls or excessive incoming calls from the same calling number
- Wangiri trigger monitoring for origination calls to high termination rate destinations with short duration (to trigger end-users to call back) for all calls over a 5-minute duration
- Analysis of recent and past Call Detail Records (CDRs) to benchmark against expected trends

STIR/SHAKEN Implementation

Provider has acknowledged to CORE Networks that it is currently authenticating and verifying with STIR/SHAKEN voice traffic that originates and terminates on our network.

CORES registration

CORE Networks has reviewed its CORES registration and confirmed that the information is up to date.