



Robocall Mitigation Program Description

Company Legal Name: OMNINET LTD.

FRN: 0037896552

Provider Types: Voice Service Provider, Gateway Provider

Date of Publication/Last Update: 2026-01-15

1. Introduction & Commitment

OMNINET LTD. ("the Company") is committed to preventing illegal robocalls from originating on or transiting its network. This Robocall Mitigation Program Description outlines the policies, procedures, and network safeguards we have implemented to comply with the Federal Communications Commission's (FCC) rules under 47 CFR § 64.6300 et seq., the TRACED Act, and related enforcement advisories, including those specified in DA 24-73.

2. Robocall Mitigation Practices (47 CFR § 64.6305(d)(ii), (e)(ii), (f)(ii))

The Company employs a multi-layered approach to mitigate illegal robocalls, which includes:

- **STIR/SHAKEN Implementation:** The Company fully implements the STIR/SHAKEN framework on its IP-based networks. We sign calls with appropriate attestation levels (A, B, or C) as defined by ATIS standards to validate the caller ID for terminating providers.
- **Network-Level Call Analytics & Blocking:** We utilize a combination of proprietary and third-party call analytics solutions to monitor call traffic in real-time. This system analyzes calling patterns, volumes, and other signaling data to identify, flag, and block traffic that exhibits characteristics of illegal robocalling.
- **Know Your Customer (KYC) Procedures:** We maintain robust customer identification and vetting procedures for all new customers, particularly those purchasing bulk originating services. This includes verifying identity and assessing the risk profile of potential customers. Especially for Greek customers we have implemented the KYC procedure provided by the Greek Authorities. For European companies we are additionally checking their Vies data.
- **Contractual Prohibitions & Enforcement:** Our terms of service explicitly prohibit the origination or transmission of illegal robocalls. We reserve the right to monitor traffic and suspend or terminate service to any customer found to be originating illegal robocall traffic.
- **Traffic Monitoring & Anomaly Detection:** We continuously monitor network traffic for sudden spikes, irregular calling patterns, and other anomalies that may indicate robocall campaigns.
- **Cooperation with Traceback Requests:** The Company commits to fully and promptly cooperating with all lawful traceback investigations initiated by the Industry Traceback Group (ITG), law enforcement, or the FCC to identify the source of illegal robocalls.

3. Practices to Prevent Illegal Robocall Originators from Using Its Network to Originate Calls (47 CFR § 64.6305(d)(iii), (e)(iii), (f)(iii))

Specifically, to prevent our network from being used to originate illegal robocalls, the Company:

- **Implements Strict Origination Point Controls:** We restrict which customers and from which network points are authorized to originate calls, especially for high-volume services.
- **Requires Robocall Mitigation Compliance for Partners:** We require all upstream providers and partners that originate traffic onto our network to have and enforce their own robocall mitigation programs, including STIR/SHAKEN implementation where applicable.
- **Investigates Consumer Complaints:** We monitor and investigate complaints received via our own channels, the FCC, or industry complaint forums regarding unwanted calls originating from our network.
- **Takes Prompt Mitigation Action:** Upon identifying a customer as a source of illegal robocalls—through analytics, traceback, or credible complaint—we take immediate action which may include throttling, blocking, or terminating the customer's service.
- **Maintains an "Opt-In" for New Customers:** For certain high-risk services, we may require a manual review and approval process before allowing new customers to originate traffic.

4. Filing Instructions Public Notice (DA 24-73) Compliance

In accordance with the FCC's guidance in DA 24-73, this description:

- Is publicly available on our website at: <https://www.omninet.gr/robocalls>
- Is written in clear, plain language describing specific practices.
- Is submitted in the appropriate provider category in the Robocall Mitigation Database.
- Affirms that the practices described are operational and actively enforced.

5. Program Administration & Review

This Robocall Mitigation Program is under the oversight of our Network Security Team. The program is reviewed and updated at least annually, or more frequently as required by changes in regulations, industry standards, or emerging robocall threats.

6. Contact Information for Robocall Mitigation Inquiries

For questions related to this program, traceback requests, or suspected illegal robocall traffic, please contact:

Designated Contact: Compliance Manager

Email: compliance@omninet.gr

Phone: +30 212 213 1020