

Robocall Mitigation Plan

1. Purpose and Scope

This Robocall Mitigation Plan describes the measures implemented by the Company to prevent, detect and mitigate unlawful, fraudulent and abusive voice traffic, including illegal robocalls, in accordance with the requirements of the Federal Communications Commission.

The Plan applies to all voice traffic transmitted through the Company's network, including traffic that may originate from, transit through, or be terminated to the United States. Depending on the specific service configuration, the Company may act as a transit provider and/or gateway provider for voice traffic involving the United States. The mitigation measures described in this Plan are applied consistently with the Company's role in the call path.

2. Traffic Monitoring and Detection

The Company operates an internal anti-fraud and traffic monitoring system designed to perform continuous real time analysis of call activity across its network.

The system monitors call signaling and traffic parameters, including call attempt rates, call setup behavior and destination patterns, in order to identify potentially unlawful, suspicious or abusive traffic.

The monitoring system is configured to detect traffic patterns commonly associated with fraudulent or automated calling activity, including but not limited to:

- multiple call attempts to the same destination number within a short time period;
- simultaneous or repeated calls to the same B number from one or multiple sources;
- abnormal volumes of call attempts or call setup rates;
- traffic behavior indicating artificially generated or automated calls.

3. Mitigation Actions

When suspicious traffic is identified, the anti-fraud system generates real time alerts and applies automated mitigation measures based on predefined risk thresholds.

Mitigation measures may include, but are not limited to:

- temporary suspension of the relevant traffic flow;
- rate limiting of call attempts;
- blocking of specific source identifiers, routes or call streams.

Mitigation actions are applied promptly to reduce the risk of unlawful robocalls and protect the integrity of the network.



VIVALDI TELECOM LTD/ ВИВАЛДИ ТЕЛЕКОМ ЕООД
Unique Identification code: 205227648
VAT: BG205227648
2 GOLASH STREET 1000 DISTRICT OF SLATINA SOFIA BULGARIA
Tel.+ +359 2491 7067
www.vivalditele.com

4. Investigation and Enforcement

All detected incidents and applied mitigation actions are logged and subject to internal review by the Company's operational staff.

If traffic is confirmed to be fraudulent, unlawful or abusive, the Company reserves the right to permanently block the originating source and to suspend or terminate services associated with such traffic in accordance with its contractual terms and Acceptable Use Policy.

The Company cooperates with downstream carriers and partners as reasonably required to address confirmed cases of unlawful robocall activity.

5. Ongoing Review and Updates

The Company regularly reviews and updates its traffic monitoring rules, fraud detection logic and mitigation thresholds to ensure continued effectiveness and compliance with applicable regulatory requirements.

This Robocall Mitigation Plan is maintained as an active operational document and reflects the Company's current procedures for preventing and mitigating illegal robocalls.

6. STIR/SHAKEN Status

The Company's network infrastructure is fully compatible with the STIR/SHAKEN framework and is capable of securely transporting SIP calls that are already authenticated and signed by upstream carriers, without modifying, stripping, or invalidating STIR/SHAKEN Identity headers.

The Company does not perform call signing directly on its own infrastructure. Instead, call authentication is performed by its upstream origination and termination partners, who are fully STIR/SHAKEN-enabled and authorized to apply attestation.

The Company maintains documented procedures to support appropriate attestation levels. Where A-level attestation is required, the Company obtains Direct Inward Dialing (DID) resources directly from its upstream provider. Where B-level attestation is applicable, the Company provides its upstream partners with a list of purchased DIDs along with supporting documentation confirming ownership and right-to-use.

The Company's network also includes technical controls capable of identifying calls that are not authenticated under STIR/SHAKEN. Where calls cannot be signed by upstream partners for technical or operational reasons, the Company has the ability to restrict, rate-limit, or block such unsigned traffic based on risk assessment, destination requirements, or partner policies.



VIVALDI TELECOM LTD/ ВИВАЛДИ ТЕЛЕКОМ ЕООД

Unique Identification code: 205227648

VAT: BG205227648

2 GOLASH STREET 1000 DISTRICT OF SLATINA SOFIA BULGARIA

Tel.+ +359 2491 7067

www.vivalditele.com

For any traffic not fully covered by STIR/SHAKEN authentication, the Company applies the robocall mitigation measures described in this Plan in accordance with 47 CFR § 64.6305.

7. Traceback Cooperation and Response Obligations

The Company commits to responding fully and in a timely manner, and in any event within twenty-four (24) hours, to all traceback requests received from the Federal Communications Commission, law enforcement agencies, upstream or downstream carriers, and the Industry Traceback Group.

The Company cooperates with such entities in investigating, mitigating, and preventing illegal robocalls and related fraudulent or abusive calling activity, in accordance with the requirements set forth in 47 CFR § 64.6305(a) and 47 CFR § 64.6305(b).

Upon receipt of a traceback request, the Company undertakes reasonable efforts to identify the source of the relevant traffic, review associated call records, and take appropriate mitigation or enforcement actions, including traffic restriction, blocking, or service termination where warranted. Traceback requests are handled by designated operational and compliance personnel.

8. KYC Procedure

The Company performs customer due diligence prior to enabling voice services. Customer onboarding includes verification of identity and business information, review of intended traffic use cases, and assessment of potential robocall or fraud risk. The Company does not knowingly provide service to customers engaged in illegal robocalling or other abusive calling practices.