



ROBOCALL MITIGATION PLAN

Date: 25.02.2026.

STELECOM SOLUTIONS SPLL (“the Company”) is a Bulgarian provider that carries and processes telecommunications traffic that transits, or is expected to transit, the public switched telephone network (PSTN). The Company does not originate calls to end users and does not terminate calls to end users.

To reduce the risk that the Company’s network is used to transmit or facilitate illegal robocall traffic, the Company maintains and enforces the following mitigation measures:

- **Continuous network surveillance and automated fraud detection**
The Company operates 24/7 traffic oversight using a centralized Fraud & Risk Monitoring Platform that evaluates signaling and call patterns in near real time. The platform detects suspicious activity, including (without limitation) robocalling, short-duration high-volume burst patterns, Wangiri/one-ring activity, PBX compromise, IRSF, artificially inflated traffic, spoofing indicators, and spam campaigns. Alerts are escalated for analyst review, and corrective actions are taken.
- **Rapid response to traceback requests and collaboration with enforcement and industry partners**
The Company maintains a designated compliance contact and internal escalation path to acknowledge, investigate, and respond promptly to traceback inquiries from the FCC, law enforcement, and the applicable industry traceback consortium.
- **Risk-based onboarding, KYC**
Prior to enabling service, the Company applies a Know Your Customer (KYC) and counterparty due diligence process proportionate to the customer’s risk profile.
- **Robocall Mitigation Database (RMD) gating**
The Company permits traffic that presents U.S./NANP caller ID information only where the responsible customer (and/or the originating voice service provider, as applicable) can demonstrate appropriate authorization and compliance, including maintaining a current and valid listing in the FCC Robocall Mitigation Database.
- **Contractual safeguards and acceptable use rules**
Customer and vendor agreements prohibit the use of the Company’s services for unlawful calling, spoofing, or the transmission of illegal robocalls, and require cooperation with traceback and fraud investigations (including identifying relevant upstream providers). The Company reserves the right to apply call blocking, suspension, or termination for non-compliance, failure to cooperate.