

Robocall Mitigation Program
of
Telroaming Advanced Communication Solution Ltd.

June 2026

Telroaming Advanced
Communication Solution Ltd.
240 Kent Ave., Suite B7A
Brooklyn, NY 11249

I. Introduction

Pursuant to the applicable orders and regulations of the Federal Communications Commission (“FCC” or “Commission”), this Robocall Mitigation Program (“RMP”) details the procedures of Telroaming Advanced Communication Solution Ltd. (“Telroaming”) to prevent unlawful robocalls from originating, terminating, or being carried or processed where Telroaming is operating as a Voice Service Provider. Unless defined differently herein, capitalized terms used herein have the same definitions as set forth in 47 C.F.R. § 64.6300.¹

A. Company Summary

Telroaming operates exclusively as a non-facilities-based mobile virtual network operator Small Voice Service Provider, as defined, with a correspondingly limited STIR/SHAKEN implementation obligation as further noted herein. Telroaming is owned by a non-U.S. entity and has received international 214 authority from the Commission, does not fall under the foreign voice service provider definition of 47 C.F.R. § 64.6300(c), and is not an intermediate or gateway provider.

Telroaming does not have an Operating Company Number (“OCN”) and does not have direct access to telephone numbers from the North American Numbering Plan Administrator (NANPA) and/or the National Pooling Administrator. If Telroaming obtains an OCN it will secure a Service Provider Code token that will be used to authenticate calls and will amend this Plan and officer certification, as necessary.

B. Filing of RMP and Implementation of STIR/SHAKEN

Telroaming certifies that it has not been prohibited from filing in the Robocall Mitigation Database. Telroaming certifies that it independently reviews underlying carrier subscriber traffic analytics and does not currently engage a third-party analytics provider. Telroaming certifies further that it has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing, and at no time during the prior two years has Telroaming been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

¹ Telroaming has implemented rules established under the FCC’s *Sixth Report and Order* along with its *Seventh Report and Order* and *Eighth Report and Order*. See *Call Authentication Trust Anchor*, WC Doc. No. 17-97, Eighth Report and Order, FCC 24-120 (rel. Nov. 22, 2024) (“*Eighth Report and Order*”); *Advanced Methods to Target and Eliminate Unlawful Robocalls*; *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Seventh Report and Order, FCC 23-37, at Appendix A (rel. May 19, 2023) (“*Seventh Report and Order*”); *Advanced Methods to Target and Eliminate Unlawful Robocalls*; *Call Authentication Trust Anchor*, WC Doc. No. 17-97, Six Report and Order and Notice of Proposed Rulemaking, FCC 23-18, at Appendix A (rel. Mar. 19, 2023) (“*Sixth Report and Order*”).

Pursuant to Section 64.6305 of the Commission’s rules, 47 C.F.R. § 64.6305, Telroaming commits to take all such reasonable steps to avoid originating illegal robocall traffic including a commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement agencies, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers/robotexters that use its service to originate calls. As set forth below, Telroaming has adapted the North America Numbering Council Call Authentication Trust Anchor Working Group’s *Best Practices for the Implementation of Call Authentication Frameworks*² into its Plan.

As a non-facilities-based mobile virtual network operator service provider, Telroaming must defer to its underlying carriers regarding interconnection with upstream providers, and its underlying carriers’ analytics to block illegal traffic that may originate with upstream providers. Telroaming thus has “not implemented the STIR/SHAKEN authentication framework on any portion of its network” because it is “unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN.”³

Pursuant to 47 C.F.R. § 64.6305(d)(2)(ii) and (iii), Telroaming’s RMP, which has been uploaded into the RMD, reflects the “reasonable steps to avoid originating illegal robocall traffic” and includes “a commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.”

Pursuant to 47 C.F.R. § 64.6305(d)(4)(vi)(3), Telroaming’s role in the call chain includes being Voice Service Provider without a STIR/SHAKEN implementation obligation serving end-users.

In accordance with 47 C.F.R. 64.6305(d)(2)(iv), Telroaming states that that during the past two years, it (and/or any entity with which Telroaming shares common ownership, management, directors, or control) has not been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient RMD certification or RMP description.

II. Robocall Mitigation Program

This RMP applies to Telroaming’s services and provides information on the specific reasonable steps Telroaming has taken to avoid originating, terminating, or carrying or processing illegal robocall traffic:

Subscriber Vetting

Telroaming telecommunications service subscribers will be commercial enterprises. Telroaming fully vets each subscriber before providing service to the subscriber. Telroaming

² *Public Notice*, WC Docket Nos. 17-97 and 20-324, DA 20-1526, Appendix B (December 22, 2020)

³ 47 C.F.R. § 64.6305(d)(2)(i).

obtains specific subscriber information, including service locations and principals. Further, Telroaming compares information provided by the subscriber to underlying carrier records to verify accuracy and authentication and to validate subscriber information. Subscribers are served under a service agreement.

Telroaming has some capability to monitor subscriber traffic for call, originating number and terminating number irregularities in conjunction with its underlying carriers; should irregularities be discovered, Telroaming will promptly contact the subscriber as part of Telroaming's investigatory process.

Telephone Number Validation

Telroaming will ensure that only those subscriber telephone numbers held by its subscribers may originate traffic. For toll-free numbers, Telroaming will verify the underlying ten-digit numbers and ensure that only calls from the assigned numbers may originate calls.

Network Traffic Monitoring, Analysis and Investigation

Consistent with the above commitments, Telroaming will respond fully to all traceback requests from the Commission, law enforcement, and the industry traceback consortium as soon as possible and at no time exceeding 24 hours from the time of the request, and will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

As a non-facilities-based voice service provider, Telroaming coordinates with its underlying carriers to monitor Telroaming subscriber traffic and identify and investigate traffic anomalies, such as unusually high call volumes to different telephone numbers and disparate geographic areas over the course of one or more hours, and will promptly block subscriber service if robocalling is suspected. Telroaming does not separately engage a third-party analytics vendor. Confirmation of illegal activity and more than one violation will result in immediate subscriber service termination.

Refusing Traffic from Unlisted Providers

In conjunction with its underlying carriers, Telroaming refuses to accept traffic from unlisted and de-listed providers in the Commission's Robocall Mitigation Database.

Ongoing Robocall Mitigation

Telroaming, in conjunction with its underlying carriers, will implement a call authentication protocol for voice calls delivered over the non-IP portions of its network that do not use SIP technology when such a protocol is fully developed and finalized by industry standards and the necessary equipment and software is available on the commercial market.

Telroaming anticipates that its Plan will evolve as it makes Plan enhancements, as underlying carriers enhance their own plans, and as the Trust Anchor and industry gain experience in caller ID authentication protocols. Telroaming coordinates such efforts with its underlying carriers, including utilization of reasonable do-not-originate lists.

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), Telroaming will update its submission in the RMD within ten business days of any change to the requisite information.

Designation of Employee Responsible for Addressing Robocall Mitigation-Related Issues

To further ensure Telroaming's network is not utilized for the origination, termination, carrying or processing of unwanted and illegal robocalls, Telroaming provides the following information for the individual within Telroaming who handles robocall mitigation-related issues and responds to traceback inquiries from the FCC, ITG, and law enforcement agencies:

Contact Name:	Evan Saltzman
Contact Title:	GRC Manager
Contact Street Address:	240 Kent Ave., Suite B7A
Contact City:	Brooklyn
Contact State and Zip Code:	NY 11249
Contact Telephone Number:	+972-73-289-7102
Contact Email:	evan.saltzman@iamwebbing.com

Employee Training

Finally, it is Telroaming's policy that employees responsible for combating robocalling are educated on the Telroaming RMP along with any related implementing procedures and are appropriately apprised of the latest developments and emerging trends to combat illegal robocalling. Telroaming treats this continuing education as an important component of its role in the telecommunications ecosystem and as a partner in mitigating illegal traffic.

* * *