



Aovataalk™

ROBOCALL

MITIGATION PLAN

Aovataalk Communications Limited

UNIT 1603, 16TH FLOOR, THE L.PLAZA 367 -
375 QUEEN'S ROAD Sheung Wan HK 999077

Pursuant to 47 C.F.R. § 64.6305 Aovataalk Communications Limited submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This report describes the status of its implementation of STIR/SHAKEN and the practices and procedures Aovataalk Communications Limited (hereinafter also referred to as "The Company") has in place to mitigate illegal robocalls as of **February 19, 2026**. The Company may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time to respond to changes in its business, its capabilities and its needs and will update its filing within 10 business days when changes occur.

As a foreign voice service provider, the Company does not maintain its own SPC token and therefore does not originate STIR/SHAKEN authentication using a Company-issued signing certificate. Because the Company is incapable of obtaining an SPC token due to Governance Authority policy, it is exempt from the voice service provider call authentication requirements in 47 CFR § 64.6301 until it is capable of obtaining an SPC token, pursuant to 47 CFR § 64.6304(b). Accordingly, the Company relies on its U.S.-based gateway and downstream providers to apply STIR/SHAKEN authentication where required and technically feasible, and the Company maintains and enforces a robust robocall mitigation program (including KYC, traffic monitoring, prompt investigation, and suspension/termination of suspicious traffic) as described below.

Aovataalk Communications Limited is judiciously working to prevent unlawful robocalls from originating on its network and has implemented the following robocall mitigation plan to address unlawful robocall traffic.

Aovataalk Communications Limited has enforceable terms of use and/or an acceptable use policy noted in its contracts. These policies define the circumstances by which the company will deny, suspend, or terminate service to a customer. We have a vetting and review process for potential customers and periodic review of customer accounts.

The Company confirms that its downstream/interconnecting providers maintain current certifications in the FCC Robocall Mitigation Database. The Company will not establish or continue interconnection arrangements that involve the exchange of voice traffic with a

provider that is not properly registered, as applicable. The Company also complies with its downstream/interconnecting providers' onboarding and due diligence requirements and has provided the KYC documentation they require from the Company.

Aovataalk Communications Limited downstream carriers are;

[REDACTED]

Aovataalk Communications Limited follows the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group. This process includes the collection and review of entity-identifying information to confirm that Aovataalk Communications Limited has an authenticated relationship with the customer. The Company uses this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

Aovataalk Communications Limited also thoroughly vets all customers utilizing our proprietary dialer and VoIP services by conducting background checks and verifying the legal documentation for the campaigns they are running. The company also requires customers to use our dialing and VoIP service.

Aovataalk Communications Limited contractual provisions with customers prohibit them from initiating illegal robocalls. If the Company discovers a customer is initiating suspicious robocalls, it warns them to stop. If such traffic continues, then the Company terminates their service.

Aovataalk Communications Limited takes the following measures to weed out end users that could potentially generate robocall traffic:

The Company uses a KYC to confirm the following information for its customers:
[REDACTED]

When the customer is a business, Aovataalk Communications Limited also requires Business Incorporation Documents and verifies they have a reputation as a valid business that abides by the law.

Aovataalk Communications Limited uses [REDACTED].

The software provides detailed reporting to identify suspected illegal robocalls. The system alerts us if we process outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list. The Company will immediately investigate any identified suspicious calls to determine if the caller was attempting to originate unlawful robocalls. If the Company determines that the traffic was likely unlawful, then we warn them to stop making such calls. If they continue the activity that appears to be unlawful, then we terminate their service.

Aovataalk Communications Limited will comply fully with all conditions set forth by the FCC, as well as with the Commission's rules and policies more generally.

Aovataalk Communications Limited has designated a dedicated point of contact for addressing traceback requests from the registered traceback consortium (the Industry Traceback Group, "ITG"), the Federal Communications Commission ("FCC"), and law enforcement. The Company has provided the ITG with current contact information for this point of contact. Aovataalk Communications Limited will respond within 24 hours to all traceback requests from the ITG, the FCC, and law enforcement, and will cooperate with such entities in investigating and stopping suspected illegal robocalls. If a traceback indicates suspicious or potentially unlawful calling activity, Aovataalk Communications Limited will take appropriate mitigation action, which may include investigation, suspension, blocking, and/or termination of the responsible customer or traffic, consistent with applicable law and the Company's contractual rights. Aovataalk Communications Limited will also provide law enforcement and regulatory agencies with relevant non-proprietary information in response to reasonable and legitimate requests concerning suspected illegal robocalls and related suspicious activity, and will implement required robocall mitigation measures to the fullest extent practicable with the goal of maximizing mitigation of illegal robocalls.

Aovataalk Communications Limited performs the same mitigation steps for all outbound calls.

Aovataalk Communications Limited does not wish to publicize any private and/or classified information that has the potential to expose the Company to fraud and/or anti-competitive actions. Therefore, the Company will submit a redacted version for the public site and requests that the FCC keep the unredacted version CONFIDENTIAL.
