

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN

Pursuant to 47 C.F.R. § 64.6305, Knowlarity Communications Holdings Pte. Ltd. (“Company”) submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal calls. Company reserves the right to modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time as it deems appropriate to reflect its business, its capabilities, and its needs.

Company Background

Knowlarity Communications Holdings Pte. Ltd. is a Singapore-incorporated cloud communications platform (Communications Platform as a Service – CPaaS) providing enterprise-grade voice communication solutions to verified business customers. Company’s platform supports programmable Voice APIs, Hosted Interactive Voice Response (IVR), Enterprise SIP Trunking, Direct Inward Dialing (DID) / Virtual Mobile Number (VMN) provisioning, WebRTC, and cloud contact center capabilities integrated with enterprise CRM systems.

Company provides voice services exclusively to legitimate enterprise organizations under strict commercial agreements. Its primary customer base spans regulated and enterprise sectors, including Banking & Financial Services, Insurance, Healthcare, E-commerce, Logistics, Retail, Technology, Education, Hospitality, Government (where applicable), and Business Process Outsourcing (BPO). Company does not knowingly serve high-risk consumer telemarketing entities or facilitate unlawful robocalling, fraudulent caller ID spoofing, phishing, or unverified voice traffic.

STIR/SHAKEN Implementation

As a foreign voice service provider, Company is not subject to 47 C.F.R. § 64.6301, *et seq.*, or 47 C.F.R. § 64.6302, *et seq.*, including the requirements in § 64.6301(a) and § 64.6302 to implement the STIR/SHAKEN call authentication framework and authenticate caller identification information. Said differently, because Company is a foreign voice service provider, the FCC does not have direct jurisdiction over the entity and cannot directly impose its STIR/SHAKEN implementation obligations upon it. The FCC recognized this lack of direct jurisdiction over foreign entities in paragraph 7 of its May 2022 Gateway Provider Order (FCC 22-37). More recently, the FCC explicitly acknowledged that foreign voice service providers are not required to implement STIR/SHAKEN in paragraph 15 of its July 2026 Robocall Mitigation Database Further Notice of Proposed Rulemaking (FCC 26-49). While Company has not implemented STIR/SHAKEN, it has implemented a robocall mitigation plan for its calls, as described below.

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that Company has implemented to detect and prevent unlawful, fraudulent, or otherwise prohibited calling activity. The measures described below explain how Company mitigates and addresses the risk that it will transmit illegal traffic in some capacity. Company will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should it determine that changes are appropriate, it will update its practices.

Customer and Upstream Provider Due Diligence

- Company conducts a comprehensive due diligence review of new and renewing customers and any upstream providers with which it interacts. This includes collecting, maintaining, and verifying information sufficient to confirm the customer's or upstream provider's identity (e.g., name, physical address, telephone number, email address, etc.) and the intended use of Company's services. Company also assesses a customer's or upstream provider's business reputation, expected call profiles (e.g., call volume, average call duration, completion ratios), and authorized CLI usage prior to provisioning numbering resources or routing outbound U.S. traffic. Together, this information can also be used to identify these customers or providers should any unlawful activity occur.
- Company will terminate or suspend service to any customer or provider with a history of non-compliance with its contractual obligations or with Company's Terms and Conditions, including provisions relating to acceptable use of the Company's service and not using the Company's services for any unlawful purpose.

Additional Measures to Prevent or Avoid Exchanging Illegal Calls

- **Monitoring and Analytics.** Company uses internal monitoring and call analytics to identify unusual, suspicious, or potentially illegal traffic. Company uses internal systems, traffic data, call records, customer information, complaints, and applicable rules or thresholds to identify traffic that requires further investigation. Some patterns Company will monitor for include low average call duration and low call completion ratios. Upon noting any unusual, suspicious, or potentially illegal traffic, Company will investigate this traffic further to determine if the traffic relates to unlawful activity and warrants further action by the Company. Company does not currently use a third-party vendor for its monitoring or analytics. However, where applicable, Company may use third-party information, carrier notifications, traceback information, or other external sources as supplemental inputs for its internal monitoring, investigation, and mitigation processes.
- **Review of Complaints and Abuse Reports.** Company reviews customer complaints and abuse reports regarding illegal and fraudulent traffic. Company also maintains call records and related traffic information that can be used to investigate these complaints as well as any suspected fraud and potentially illegal calling activity.
- In the event fraudulent or unlawful traffic is detected, Company will take action to mitigate this traffic, including identifying and blocking such traffic, restricting unauthorized CLIs, or suspending non-compliant accounts.

Responding to Traceback Requests

- Company follows relevant Industry Traceback Group Best Practices to facilitate its response to any traceback requests, including specifically:

- **Dedicated Point of Contact** – Company has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual, and can provide the ITG with the contact information and business hours for those individuals.
- **Prompt Investigation and Response** – Upon receiving a traceback request from the FCC, law enforcement, or the ITG, Company will aim to respond to the traceback request within 24 hours of receipt of the request, to the extent permitted under applicable law.
- **Privacy of Traceback Investigations** – Company will not share information about traceback investigations, except with the ITG, the FCC, and law enforcement, and to the extent permitted under applicable law.
- Company maintains the records and processes necessary to investigate and respond to traceback requests.
- Company maintains current and correct information for its customers so that it can provide accurate responses to traceback requests.

Cooperation with State and Federal Regulators

Company will cooperate, to the extent permitted under applicable law, with valid requests from the FCC or law enforcement to identify and stop any illegal calls that are linked to Company. Specifically, consistent with applicable law, Company will:

- Respond to valid law enforcement requests;
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal calls and suspicious activities; and
- Implement robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal calls.