

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, TI Sparkle SpA and its affiliates (TI Sparkle North America, Inc. and TI Sparkle Singapore Pte. Ltd.) hereinafter “TIS” submit this plan to prevent and mitigate illegal robocalls. TIS 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, its needs and FCC obligations.

Companies Background

TIS has been in the telecommunications business since 2002 and is a leading global service provider offering a full range of infrastructure and global connectivity services – capacity, IP, SD-WAN, colocation, IoT connectivity, roaming and voice - designed to meet the fast-changing needs of national and international Carriers, OTTs, ISPs, Media/Content Providers and multinational enterprises.

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that TIS has implemented to detect and prevent illegal robocalls on its network. TIS is at risk of exchanging illegal robocalls principally if it is passed such traffic from its upstream carrier customers. The measures described below explain how TIS mitigates and addresses that risk. TIS 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, its practices may differ from those described below.

TIS, in accordance with the industry view (e.g., GSMA, i3Forum), does not view robocalls in general as a type of fraud and its approach to detection and mitigation of illegal robocalls, as potential driver of fraud attempts, relies in large part on TIS anti-fraud practices and protections. TIS vigorously monitors its traffic for signs of fraud. When potential fraud is detected or when fraud is reported to TIS, TIS will investigate the source and circumstances of the traffic and will implement measures to block such traffic from recurring on its network. TIS works with a variety of industry stakeholders, including the Industry Traceback Group (ITG), the i3Forum, and CBAN, to prevent fraud, including illegal robocalling.

Customer Due Diligence / Knowing Upstream Carriers

- TIS conducts a comprehensive due diligence and credit review before establishing a contractual relationship with carrier customers.
- TIS researches its carrier customers’ reputation and assesses the accuracy of all reported information, including physical business location, contact person(s), state or country of incorporation, and the nature of the business.
- TIS collects sufficient information to verify customer information is current when contracts are renewed or services are added.

- TIS will terminate or suspend service to customers with a history of non-compliance with its contractual obligations, including provisions relating to acceptable use of TIS service. Further information is provided below.

Additional Measures to Prevent or Avoid Exchanging Illegal Robocalls

- **Contractual Provisions** – TIS contracts typically establish a reciprocal general obligation between TIS and its carrier customers to not use the services for any unlawful purpose, to prevent fraudulent uses, and to cooperate with each other to avoid these unlawful activities. TIS contracts also include a fraud clause, which follows the i3Forum model and stipulates the legal actions TIS can take in case of receiving fraudulent traffic. The clause establishes: (1) the definition of what constitutes fraud; (2) liability and payment rules when fraud is found; (3) a right to suspend service; (4) the ability to initiate a dispute and dispute resolution procedures; and (5) credit note handling principles.
- **Fraud Detection** – TIS is fully engaged in the fight against illegal robocalling, CLI spoofing as a means to engage in fraud. TIS has created inter-working groups with the participation of stakeholders from several departments, including Security, Engineering, Product Management, Operations and Legal, in order to develop and support activities to mitigate illegal robocalling, spoofing and other fraud. TIS representatives participate in international anti-fraud forums, including the i3Forum and CBAN, to share information and employ best practices for countering robocalling and CLI spoofing. The TIS anti-fraud group functions 24 hours a day, 7 days a week and manages the search and detection of fraudulent traffic as well as escalation and notifications when such traffic is identified.
- **Blocking** – TIS blocks traffic from invalid numbers, including when the ITG provides evidence or a report. TIS also will block traffic that appears to be illegal or is flagged as suspicious under its fraud policy, and any traffic that the FCC requires to be blocked. TIS currently relies on internal and external reports rather than an analytics system to identify and block illegal traffic. Therefore, TIS does not use a third-party analytics vendor.
- **Do-Not-Originate (DNO) List Blocking** – As a U.S.-based provider, TI Sparkle North America, Inc. has adopted and is blocking calls based on a reasonable DNO list. The DNO list on which TI Sparkle North America, Inc relies includes the types of numbers which the FCC identified in its 8th Report and Order in CG Docket No. 17-59 (FCC 25-15).

Responding to Traceback Requests

- TIS participates in the ITG.
- TIS follows the relevant ITG Best Practices to facilitate its response to traceback requests, including specifically:

- **Dedicated Point of Contact** – TIS has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual, and has provided the ITG with the contact information and business hours for those individuals.
 - **Ongoing Coordination** – TIS will coordinate with the ITG and other voice service providers in relation to instances of suspicious traffic, including exchanging information related to such traffic and ad hoc follow-up as appropriate.
 - **Prompt Investigation and Response** – Upon receiving a traceback request from the ITG, TIS will endeavor to initiate investigation of the source of suspicious traffic within four (4) business hours after receiving a traceback request and strive to complete the investigation and response to the request through the traceback portal within 24 hours. In the event TIS is unable to respond to a traceback request, it will provide sufficient information in the traceback portal as to why it is unable to respond.
 - **Privacy of Traceback Investigations** – TIS will not share information about traceback investigations, except with the ITG, with other providers involved in the traceback investigation, or when pursuant to a valid legal process.
- TIS maintains current and correct information about its upstream carrier customers so that it can provide accurate responses to traceback requests.
 - TIS performs preventive blocking of calls to U.S. destinations by providers listed as “non-responsive” by the ITG. TIS also performs blocking of calls to U.S. destinations by providers on the ITG “blacklist.”
 - TIS will periodically review records of traceback requests to identify customers that are the subject of repeated traceback inquiries. TIS will determine an appropriate action to take on a case-specific basis, which may include working with the customer to mitigate illegal traffic, temporary suspension of the customer and/or termination of the customer’s service.
 - TIS maintains records of any traceback request it receives and the carrier customer involved in the request.

Cooperation with State and Federal Regulators

TIS will cooperate with state and federal regulators to prevent illegal robocalls. Specifically, TIS will:

- Respond to requests for information about illegal robocalls;
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and

- Implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.