

TELECOM LLC

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, Telecom LLC, “Telecom”) submit this report, on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. Telecom 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

Telecom is a competitive local exchange carrier (“CLEC”) offering telephony services and authorized to provide service in 50 states and the District of Columbia. Telecom provides services to business customers and offers a variety of technology solutions to business and enterprise customers, including solutions that incorporate interconnected VoIP and cloud services.

Telecom utilizes IP networks and has implemented the STIR/SHAKEN framework. As described below, Telecom has implemented a Robocall Mitigation Program for its entire operation and Telecom has deployed protections designed to ensure that it remains free of illegal robocalls on its network.

STIR/SHAKEN Implementation

Telecom will comply fully with all conditions set forth in the FCC’s orders, rules, and policies regarding the implementation of the STIR/SHAKEN framework.

Telecom is implementing STIR/SHAKEN through use of the TNS Call Guardian Authentication Hub. This is a managed end-to-end call authentication solution that fully satisfies the FCC’s STIR/SHAKEN requirements. It provides a standardized approach to call authentication and verification (STIR – RFC 8224, RFC 8225, RFC 8226 and SHAKEN – ATIS- 1000074-E, ATIS-1000080, ATIS-1000082).

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that Telecom has implemented to detect and prevent illegal robocalls from originating on its network. Telecom is not a significant source of illegal robocalls and has tailored its robocall mitigation practices to address the areas most at risk of - originating illegal robocalls. The measures described below explain how Telecom mitigates and addresses the risk it experiences. Telecom 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.

Customer Due Diligence

- Telecom conducts a comprehensive due diligence and review before establishing a contractual relationship with customers. Telecom will review information about new and renewing customers including, but not limited to type of business, state and country of incorporation as contracts are entered into or renewed. Telecom will identify customers it believes warrant further investigation based on factors that indicate they may be capable of originating illegal robocalls, such as having been subject to a traceback request or previous robocall enforcement action. This review will be aided by external sources and internet searches as are useful in the process. If the investigation raises a concern, Telecom's account team, will discuss the concerns with the customer and take steps to ensure the customer is aware of and will abide by the restrictions. Telecom will monitor these customers on a "watch list" to determine if additional actions are necessary. Customers who do not engage in problematic practices after a period of time will be removed from the watch list.
- Telecom monitors all of its services for violations of its Terms of Service (ToS), including excessive use.
- Telecom will terminate or suspend service to customers with a history of non-compliance with its contractual obligations, including provisions relating to acceptable use of the service.

Measures to Prevent or Avoid Exchanging Illegal Robocalls

Telecom will prevent the origination of illegal robocalls on its voice network and assist with tracing and stopping illegal robocalls originating on other service providers networks. This is achieved through:

- **Contractual Provisions** – Telecom's service agreements, and Terms of Service prohibit unlawful uses of service and provide for suspension and/or disconnection for violations of these provisions. Subscribers have an obligation not to use the services for any unlawful purpose, not to engage in any fraudulent uses, and to cooperate with Telecom in mitigating unlawful activities. In addition, Telecom's contracts require subscribers to cooperate with the Company to investigate reports of unlawful activity, including cooperating with traceback requests.
- **Robocall Monitoring Procedures.** Telecom uses TNS Call Guardian analytics technologies and services to monitor traffic on its network and identify potentially unlawful call origination. TNS provides reputation monitoring of originating numbers of Telecom customers and enables Telecom to identify changes in the reputation score and suspicious activity. Telecom has developed a process to investigate incidents identified by this process. The investigation will include determination if the calls are originating on the Telecom network (or, for example, are the result of third parties spoofing numbers associated with Telecom subscribers or have been the subject of previous traceback requests) and will conduct appropriate follow-up with subscribers to remedy any problems or mitigate the situation. If effective action is not taken, Telecom can suspend and/or terminate service to the subscriber.
- **Call Center Solutions.** Telecom offers enterprise level services to call center customers offering inbound and outbound services. Telecom requires its call center customers, who serve well known, reputable brands, to adhere to applicable legal requirements, including robocall restrictions. Upon

receipt of any claim of violations of the robocalling restrictions, Telecom will address the complaint with the customer and require the customer to take appropriate remedial action if necessary.

- **Preventing Calling Line ID (CLID) “Spoofing.”** Telecom does not assist or enable its customers to “spoof” telephone numbers on the services it provides. To the extent a subscriber has customer premises equipment that enable spoofing, Telecom has no involvement in such activity. However, spoofing in violation of the Truth in Caller ID Act violates Telecom’s terms of service and is grounds for suspension and/or termination of service.
- **Call Blocking.** At this time, Telecom does not block traffic from invalid numbers by default, but is in the process of implementing analytics-based blocking service from a leading third party analytics provider. Telecom currently blocks traffic that appears to be illegal or is flagged as suspicious by its Security Team. In addition, Telecom subscribes to the National Do-Not-Originate (DNO) list and blocks calls originating from these numbers to certain subscribers.
- **Knowledge of Upstream Providers.** Telecom knows all of the upstream providers from which it directly receives traffic and has insight into its upstream providers’ policies and procedures related to identifying and blocking unlawful robocall traffic through Telecom’s review of these providers’ robocall mitigation plans. Telecom confirms that all upstream providers from which it receives traffic are listed in the FCC’s Robocall Mitigation Database.

Responding to Traceback Requests

- Telecom follows the relevant ITG Best Practices to facilitate its response to traceback requests, including specifically:
 - **Dedicated Point of Contact** – Telecom 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** – Telecom 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, Telecom 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 Telecom 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** – Telecom 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.

- Telecom maintains current and correct information about its upstream carrier customers so that it can provide accurate responses to traceback requests.
- Telecom will periodically review records of traceback requests to identify customers that are the subject of a pattern of traceback inquiries. Telecom will determine an appropriate action to take on a case-specific basis, which may include directing the customer to remedy the problem and, if effective action is not taken, temporary suspension of the customer and/or termination of the customer's service.
- Telecom maintains records of any traceback request it receives and the customer involved in the request.

Cooperation with State and Federal Regulators

Telecom will cooperate with state and federal regulators to prevent any and all illegal robocalls. Specifically, Telecom will:

- Respond to request 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.