

**INSTRUCTIONAL TELECOMMUNICATIONS FOUNDATION, INC.
D/B/A MISSION TELECOM**

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN

Pursuant to 47 CFR § 64.6305, Instructional Telecommunications Foundation, Inc. d/b/a Mission Telecom, hereafter “Company”, submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. Company reserves the right to modify, add, delete or otherwise alter any of the policies and procedures described herein at any time as it deems appropriate to reflect its business, its capabilities, its needs, and Federal Communications Commission (“FCC”) obligations.

Company Background

Company operates as a mobile virtual network operator (“MVNO”) which relies on a major carrier’s network to offer service. Company therefore lacks ultimate control over the facilities/network infrastructure necessary to implement the STIR/SHAKEN framework.

Company’s customers include non-profit organizations, educational institutions (schools and universities) and libraries, and Company’s services are used by the employees of these organizations and, in some cases, end users served by the Company’s partners.

Based on the foregoing, Company is not a significant risk of originating illegal or unwanted robocalls. Company has tailored its Robocall Mitigation Plan in light of this low risk. The specific, reasonable measures Company takes given the level of risk it faces are described in this plan.

STIR/SHAKEN Implementation

Company has not implemented the STIR/SHAKEN call authentication framework and is unable to do so. As noted above, Company is an MVNO, and it therefore lacks control over the facilities and network infrastructure necessary to implement STIR/SHAKEN. Since Company lacks this control, it is excluded from the FCC’s STIR/SHAKEN implementation obligation pursuant to paragraph 40 of the FCC’s First Call Authentication Report and Order.¹ Instead, Company relies on its underlying carrier partner, which owns and maintains the network infrastructure, to implement and utilize STIR/SHAKEN authentication.

¹ See *Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, FCC 20-42, 35 FCC Rcd 3241, 3260, para. 40 (2020).

Based on the foregoing, Company's role in the call chain is as a voice service provider without a STIR/SHAKEN obligation.

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that Company has implemented to detect and prevent illegal robocalls. As an MVNO that offers service to non-profit organizations, educational institutions and libraries, Company is not a significant source of illegal robocalls. However, the measures described below explain how Company will mitigate and address any risks it experiences. 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, its practices may differ slightly from those described below.

Know Your Customer

- Company collects and maintains information from each customer (i.e., the non-profit organization, educational institution or library) sufficient to confirm the customer's identity (e.g., name, physical address, telephone number, email address, etc.) and its intended use of Company's services. This information can be used to identify these customers should any unlawful activity occur.
- Company will monitor its services for violations of its Terms and Conditions, including using Company's services in any way that violates any applicable federal, state, local, or international law or regulation, and using Company's services to transmit spam or any other similar solicitation. Company will suspend or terminate service to subscribers with a history of noncompliance with its Terms and Conditions, including repeatedly engaging in the violations listed above.

Other Measures to Prevent or Avoid Exchanging Illegal Robocalls

- **Know Your Upstream Provider** – As an MVNO that will initiate end user calls, Company will not deal with upstream providers on the origination side of the call path. All calls will be routed through the relevant underlying carrier's network upon origination. On the termination side, Company knows the major underlying carrier which passes it traffic well (including its name, physical address, telephone number, etc.) and it enters into contracts with this well-known carrier.
- **Robocall Analytics and Blocking** – As an MVNO, Company relies on its underlying carrier partner to adopt analytics software for monitoring call traffic and to block relevant calls. Specifically, Company relies on its carrier partner's robust scam identification and scam blocking solutions. Company itself does not directly use any call analytics systems

to identify and block illegal traffic, and it does not use a third-party analytics vendor. To the best of Company's knowledge, its underlying carrier will identify and block calls from providers that have not filed in the Robocall Mitigation Database. Because such blocking will be done at the network level, Company will not have control over this as an MVNO.

- **Monitoring** – Company also monitors for call patterns that may be indicative of illegal robocalling. Upon noting any of these patterns, Company will contact relevant partners to determine if these patterns are indeed due to unlawful activity and warrant further investigation. These patterns include:
 - Large bursts of calls in a short timeframe;
 - Low average call duration; and
 - Low call completion ratios.

Responding to Traceback Requests

- Company will adhere to the following best practices to facilitate its responses to traceback requests from the FCC, law enforcement, and the Industry Traceback Group (“ITG”), including:
 - **Dedicated Point of Contact** – Company will designate an individual as a point of contact for addressing traceback requests.
 - **Ongoing Coordination** – Company will coordinate with the FCC, law enforcement, 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 FCC, law enforcement, or the ITG, Company will fully respond to the traceback request within 24 hours of receipt of the request. In the event Company is unable to respond to a traceback request, it will provide sufficient information as to why it is unable to respond. Company will continue to cooperate with these entities in further investigating and stopping any illegal robocallers attempting to use its service to initiate illegal calls.
 - **Privacy of Traceback Investigations** – Company 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.

- Company will maintain records of any traceback requests it receives, including the relevant parties involved in the requests.

Cooperation with Law Enforcement and State/Federal Regulators

Company commits to cooperating with state and federal regulators to help prevent any and all illegal robocalls. Specifically, Company 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 any new robocall mitigation procedures that are mandated, or to which Company has committed, to the fullest extent possible.