

ADVANTIX SCANSOURCE, LLC

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN

Pursuant to 47 CFR § 64.6305, Advantix ScanSource, LLC, 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 is a second line mobile virtual network operator (“MVNO”)/reseller which relies upon an upstream MVNO and a major carrier’s network in order to offer service. Company therefore lacks ultimate control over the facilities/network infrastructure necessary to implement the STIR/SHAKEN framework.

Company offers service intended for end user use and, to the best of its knowledge, end user devices are not being used to place a high volume of calls at one time.

As a result, Company views itself as not a significant risk of originating illegal or unwanted robocalls. Its services are not well suited for the origination of an overly high volume of calls. Company has tailored its Robocall Mitigation Plan in light of the low risk of illegal robocalls being originated by it. The 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 a second line MVNO/reseller, 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 will rely on its underlying carrier partner(s), 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. 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.

End User Due Diligence

- Company will obtain information from each end user sufficient to confirm the end user's identity (e.g., name, address, etc.). This information can be used to identify end users should any unlawful activity occur.
- Company will monitor its services for violations of its Wireless Service Agreement, which includes its Acceptable Use Policy. Company monitors for violations by end users such as attempting to violate any applicable laws or regulations, using Company services for fraudulent purposes, engaging in excessive use of services such as by making or receiving an abnormally high number of calls, and engaging in any other improper, illegal, or unauthorized use of Company services.
- Company will suspend or terminate service to end users with a history of noncompliance with its obligations under Company's Wireless Service Agreement, including provisions relating to acceptable use of service.

Other Measures to Prevent or Avoid Exchanging Illegal Robocalls

- **Know-Your-Upstream Provider** – As a second line MVNO/reseller involved in the origination of end user calls, Company does not deal with any upstream providers in the middle of the call chain. Company knows the first line MVNO with which it deals due to its direct contractual relationship with this MVNO and the information shared as part of this contracting process, such as the first line MVNO's name, business address, business purpose, etc.
- **Robocall Analytics and Blocking** – As an MVNO/reseller, Company will rely on its underlying carrier partner(s) to adopt analytics software for monitoring call traffic and to block relevant calls. Company itself does not 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(s) 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/reseller.

- **Monitoring** – Company will monitor for call patterns that may be indicative of illegal robocalling. These patterns include, but are not limited to:
 - Making or receiving an abnormally high number of calls; and
 - Repeatedly placing calls of an unusual duration.

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 originate 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 periodically review records of traceback requests to identify end users that are the subject of repeated traceback inquiries. Company will determine an appropriate action to take on a case-specific basis, which may include working with the end user to mitigate illegal traffic, temporary suspension of the end user, and/or termination of the end user’s service.

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.