

EXCESS TELECOM, INC.

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN

Pursuant to 47 CFR § 64.6305, Excess Telecom, Inc., hereafter “Company”, submits this report, as of February 23, 2024, 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 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.

More specifically, Company is an Affordable Connectivity Program (“ACP”) provider offering service consistent with the ACP. Company offers service intended for single-line personal use and, to its knowledge, subscriber devices are not capable of placing a high volume of calls at one time. Furthermore, Company confirms that any device it provides to its subscribers is not compatible with an automatic dialing system or software that could be used to facilitate the origination of illegal robocalls.

As a result, Company is not a significant risk of originating illegal or unwanted robocalls. Its services are not well suited to the origination of a high volume of calls. Company has tailored its Robocall Mitigation Program in light of the low risk of illegal robocalls being originated on its networks. 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 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 of August 21, 2023. As an MVNO that offers service intended for single-line personal use, Company is not a significant source of illegal robocalls. However, the measures described below explain how Company mitigates and addresses 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.

Subscriber Due Diligence

- Company obtains personal information from each subscriber sufficient to confirm the subscriber's identity and its qualification under the federal program to receive service. This information can be used to identify subscribers should any unlawful activity occur.
- Company monitors its services for violations of its Acceptable Use Policy (AUP), including connecting devices that can mass dial numbers or that enable spoofing.
- Company will suspend or terminate service to subscribers with a history of noncompliance with its contractual obligations, including provisions relating to acceptable use of service. Specifically, Company contracts and policies prohibit unlawful uses of service and provide for suspension and/or disconnection for such violations. If a subscriber is enrolled in the ACP, any suspension or disconnection here is conducted in accordance with the FCC's rules governing this program.

Other Measures to Prevent or Avoid Exchanging Illegal Robocalls

- **Know-Your-Upstream Provider** – As an MVNO that originates end user calls, Company does not deal with upstream providers. All calls are routed through its underlying carrier's network upon origination.
- **Robocall Analytics and Blocking** – As an MVNO, Company relies on its wholesale provider/underlying carrier partner 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. To the best of Company's knowledge, its underlying carrier identifies and blocks calls from providers that have not filed in the Robocall Mitigation Database. Because such blocking is done at the network level, Company does not have control over this as an MVNO.
- **Monitoring** – Company monitors for call patterns that may be indicative of illegal robocalling. Upon noting any of these patterns, Company contacts relevant partners to

determine if these patterns are indeed due to unlawful activity and warrant further investigation. These patterns include:

- o Large bursts of calls in a short timeframe;
- o Low average call duration;
- o Low call completion ratios; and
- o Large volume of complaints related to a suspect line.

Responding to Traceback Requests

- Company adheres to the following best practices to facilitate its responses to traceback requests from the FCC, law enforcement, and the Industry Traceback Group (“ITG”), including:
 - o **Dedicated Point of Contact** – Company has designated an individual as a point of contact for addressing traceback requests.
 - o **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.
 - o **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.
 - o **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 subscribers 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 subscriber to mitigate illegal traffic, temporary suspension of the subscriber, and/or termination of the subscriber’s service. If the subscriber is enrolled in the ACP, any suspension or termination here would be conducted in accordance with the FCC’s rules governing this program.
- Company maintains records of any traceback requests it receives, including the relevant parties involved in the requests.

Cooperation with Law Enforcement and State/Federal Regulators

Company certifies that it has not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action.

Furthermore, Company is not currently subject to a formal Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing, nor has it been so in the past two years. The same is true for any entities affiliated with Company.

Finally, 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.