



2150 W. Northwest Hwy, Suite 114 PMB 1004, Grapevine, TX 76051

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN

Patriot Mobile, hereafter “Company”, submits this document as its Robocall Mitigation Plan Pursuant to 47 CFR §64.6305. The Company reserves the right to modify, add, change, delete or otherwise alter any of the contents of this document at any time as it deems appropriate in order to reflect its business, its operations, and its present status in accordance with Federal Communications Commission (“FCC”) obligations.

Company Background

The Company is a mobile virtual network operator (“MVNO”) and is one of the few MVNOs that offers wireless coverage on all three major carriers. The Company, as an MVNO, relies on these major underlying carriers’ networks to offer service. Therefore, the Company lacks ultimate control over the facilities and network infrastructure necessary to implement STIR/SHAKEN.

The Company offers service which is a single-line personal use and can only be used in conjunction with an assigned mobile device. To the knowledge of the Company, single line cellular subscriber devices are not capable of placing a high volume of calls or generating High Volume Short Duration (HVSD) calls at one given time.

Additionally, the Company can attest that to its knowledge that any device it provides to its subscribers is not readily compatible with an autodial or dialer system or dialer software that could be used to make rapid succession calls which would facilitate the origination of illegal robocalls. The Company services are not well suited to the origination of a high volume of calls. Therefore, the Company is at minimal risk of originating illegal or unwanted robocalls

The Company has tailored this Robocall Mitigation Plan (and its underlying program) considering the minimal 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

Because it does not own the infrastructure, the Company has not implemented a STIR/SHAKEN call authentication framework and is not able to do so. As stated earlier in this document, as an MVNO, the Company lacks control over the facilities and network infrastructure necessary to implement STIR/SHAKEN. Since Company lacks any control over and does not have its own network, it is excluded from the FCC’s STIR/SHAKEN implementation obligation in accordance with paragraph 40 of the FCC’s First Call Authentication Report and Order.¹ The Company as a true MVNO is fully reliant upon its underlying carriers, who own and maintain their individual 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).



2150 W. Northwest Hwy, Suite 114 PMB 1004, Grapevine, TX 76051

Robocall Mitigation Plan

As stated above, given that the Company is an MVNO that offers service intended for single-line personal usage, there is minimal risk that the Company is a source of illegal robocalls. However, this Robocall Mitigation Plan explains the parameters the Company has deployed to prevent illegal robocalls. The 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

The Company's Terms and Conditions allow the Company the right to suspend and/or terminate service to any subscriber who violates the Company's Terms and Conditions including engaging in Prohibited Voice Use. Examples of prohibited voice use per the Company Terms and Conditions are as follows:

Patriot Mobile voice Services are provided solely for live dialogue between and initiated by two or more individuals for personal use. However, Patriot Mobile Service may not be used for any other purposes, including, but not limited to: monitoring services, the transmission of broadcasts, the transmission of recorded material, telemarketing, auto-dialed calls, other commercial uses, or other connections that do not consist of uninterrupted live dialogue between individuals.

Other Measures to Prevent or Avoid Exchanging Illegal Robocalls

- **Know-Your-Upstream Provider** – As an MVNO that originates end user calls, the Company does not deal with any upstream providers. All calls are routed through its underlying carriers' networks upon origination.
- **Call Blocking** – To the best of the Company's knowledge, its underlying carriers identify and block calls from providers that have not filed in the Robocall Mitigation Database. Because such blocking is done at the network level, The Company does not have control over this as an MVNO. As an MVNO, Company relies on its wholesale provider/underlying carrier partners to adopt analytics software for monitoring call traffic and to block relevant calls. The Company itself does not use any call analytics systems to identify and block illegal traffic.

Responding to Traceback Requests

- The 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:
 - **Dedicated Point of Contact** – Company has designated an email address as a point of contact for addressing traceback requests. The designated email address is compliance@patriotmobile.com
 - **Ongoing Coordination** – The Company will coordinate with the FCC, any recognized governmental agency, law enforcement, the ITG in relation to instances of suspicious traffic, including exchanging information related to such traffic and ad hoc follow-up as appropriate.



2150 W. Northwest Hwy, Suite 114 PMB 1004, Grapevine, TX 76051

- **Prompt Investigation and Response** – Upon receiving any traceback request from the FCC, any recognized governmental agency, law enforcement, or the ITG, the 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. The 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** – The Company will not share information about traceback investigations, except to an official regulatory or governing body, law enforcement or with the ITG, when involved in the traceback investigation, or when pursuant to a valid legal process.
- The Company will periodically review records of traceback requests to identify subscribers that are the subject of repeated traceback inquiries. The 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.
- The Company will maintain records of any traceback requests it receives, including the relevant parties involved in the requests for a minimum of 7 years.

Cooperation with Law Enforcement and State/Federal Regulators

The Company certifies that it has not been prohibited from entering its information in the Robocall Mitigation Database. Additionally, in the last 2 years, the Company has not been subject to a formal action or investigation by any regulatory agency, or with law enforcement based on or due to suspected unlawful robocalling or spoofing.

- The Company also commits to fully cooperating with any state and federal regulators to help prevent all illegal robocalls. And the Company will implement any new robocall mitigation practices and policies that may be required in future by any additional FCC Orders or mandated FCC guidelines.