

Robocall Mitigation Plan **Getverify LDA**

Getverify LDA (“Getverify”) submits the following Robocall Mitigation Plan in compliance with 47 CFR § 64.6305(d)(ii)–(iii). Getverify is committed to taking reasonable and appropriate steps to mitigate the transmission of automated phone calls, otherwise known as Robocalls, through its underlying carrier’s network, whether terminating to an end customer or originating from its network. Because the threat and mode of action of these calls is ever evolving, there is no single solution or mitigation strategy that would be effective for all time. As such, this plan may be modified from time to time, as circumstances warrant, to reduce and ultimately mitigate the likelihood and occurrence of such calls through its underlying carrier’s network.

Company Background

Getverify is an app-based mobile virtual network operator (“AppVNO”) which relies on the network of its underlying carrier to offer service. Getverify therefore lacks ultimate control over the facilities and network infrastructure necessary to implement the STIR/SHAKEN framework.

More specifically, Getverify offers service intended for single-line personal use and its services are not well suited to the origination of a high volume of calls. As a result, Getverify is not a significant risk of originating illegal or unwanted robocalls. Getverify has tailored its Robocall Mitigation Program in light of the low risk of illegal robocalls being originated on its networks. The reasonable measures Getverify takes given the level of risk it faces are described in this plan.

STIR/SHAKEN Implementation

Getverify has not implemented the STIR/SHAKEN call authentication framework and is unable to do so. As noted above, Getverify is an AppVNO, and therefore it lacks control over the facilities and network infrastructure necessary to implement STIR/SHAKEN. Since Getverify lacks this control, it is excluded from the Federal Communications Commission’s (“FCC”) STIR/SHAKEN implementation obligation pursuant to paragraph 40 of the FCC’s First Call Authentication Report and Order¹. Instead, Getverify relies on its underlying carrier partner, which owns and maintains the network infrastructure, to implement and utilize STIR/SHAKEN authentication.

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that Getverify has implemented to detect and prevent illegal robocalls. As an AppVNO that offers service intended for single-line personal use, Getverify is not a significant source of illegal robocalls. However, the measures described below explain how Getverify mitigates and addresses any risks it experiences. Getverify 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.

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).

Subscriber Due Diligence

- Getverify obtains the user's first name, last name, email, and phone number. The user is required to authenticate the phone number in order to proceed to the app. This information can be used to identify subscribers should any unlawful activity occur.
- Getverify monitors its services for violations of its Acceptable Use Policy (AUP), including connecting devices that can mass dial numbers or that enable spoofing.
- Getverify 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, Getverify contracts and policies prohibit unlawful uses of service and provide for suspension and/or disconnection for such violations.

Other Measures to Prevent or Avoid Exchanging Illegal Robocalls

- **Know-Your-Upstream Provider** – As an AppVNO that originates end user calls, Getverify does not deal with upstream providers. All calls are routed through its underlying carrier's network upon origination.
- **Robocall Analytics and Blocking** – As an AppVNO, Getverify relies on its wholesale provider/underlying carrier partner to adopt analytics software for monitoring call traffic and to block relevant calls. Getverify itself does not use any call analytics systems to identify and block illegal traffic. To the best of Getverify'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, Getverify does not have control over this as an AppVNO.
- **Monitoring** – Getverify monitors for call patterns that may be indicative of illegal robocalling. Upon noting any of these patterns, Getverify contacts 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;
 - Low call completion ratios; and
 - Large volume of compliants related to a suspect line.

Responding to Traceback Requests

- Getverify 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** – Getverify has designated an individual as a point of contact for addressing traceback requests.

- **Ongoing Coordination** – Getverify 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, Getverify will fully respond to the traceback request within 24 hours of receipt of the request. In the event Getverify is unable to respond to a traceback request, it will provide sufficient information as to why it is unable to respond. Getverify 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** – Getverify 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.
- Getverify will periodically review records of traceback requests to identify subscribers that are the subject of repeated traceback inquiries. Getverify 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.
- Getverify maintains records of any traceback requests it receives, including the relevant parties involved in the requests.

Cooperation with Law Enforcement and State/Federal Regulations

Getverify certifies that it has not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action. Furthermore, Getverify 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 Getverify. Finally, Getverify commits to cooperating with state and federal regulators to help prevent any and all illegal robocalls. Specifically, Getverify 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 Getverify has committed, to the fullest extent possible.