

Robocall Mitigation Program Description for REVENUE PROTECT LIMITED

REVENUE PROTECT LIMITED ("the Company"), in compliance with the Federal Communications Commission (FCC) regulations, particularly as outlined under 47 CFR § 64.6305 regarding the Robocall Mitigation Database, submits this document as the detailed description of its Robocall Mitigation Program (RMP). The program addresses the Company's status as a gateway provider, which does not implement the STIR/SHAKEN authentication framework due to the absence of an IP network in its operations.

Certification and Compliance Statement

The Company certifies that it:

- Has not implemented the STIR/SHAKEN authentication framework on any portion of its network for carrying or processing calls, as per 47 CFR § 64.6305(e)(1)(iii).
- Complies with all FCC guidelines related to robocall mitigation as outlined in 47 CFR § 64.6305, maintaining an active approach to mitigating illegal robocall traffic.

Program Details

(i) Explanation of STIR/SHAKEN Non-implementation

Given the non-IP based infrastructure of REVENUE PROTECT LIMITED, the company is unable to implement the STIR/SHAKEN authentication framework. This limitation is rooted in the reliance on traditional telecommunications technologies.

(ii) Steps for Mitigating Illegal Robocall Traffic

The Company's robocall mitigation efforts include:

- Ensuring compliance with 47 CFR § 64.6305(e)(2)(ii), by engaging with upstream providers under strict contractual agreements aimed at preventing illegal robocall traffic.
- Utilizing analytics systems to identify and block potential illegal robocall traffic, in line with 47 CFR § 64.6305(e)(2)(ii). While specific analytics vendors remain confidential, all are thoroughly vetted for FCC compliance.
- Committing to full cooperation within 24 hours to traceback requests from the FCC, law enforcement, and industry consortiums, as mandated by 47 CFR § 64.6305(e)(2)(iii).