

ROBOCALL MITIGATION PLAN

This Robocall Mitigation Plan ("RMP") describes: (1) the specific reasonable steps Total Network Technologies, LLC ("Total Network TEK") has taken to avoid carrying or processing illegal robocall traffic; (2) Total Network TEK's commitment to respond fully and within 24 hours to all traceback requests from the Federal Communications Commission ("Commission"), law enforcement, and the industry traceback consortium; and (3) Total Network TEK's commitment to cooperate with such entities in investigating and stopping any illegal robocalls that use our services to carry or process calls.

1 ENTITIES COVERED BY CERTIFICATION

The following entities are all subject to the robocall mitigation policies and procedures described in this RMP:

- Total Network Technologies, LLC (FRN: 0037706504)

For the purposes of this RMP, these entities are collectively referred to as "Total Network TEK."

2 DESCRIPTION OF ROBOCALL MITIGATION PLAN

2.1 EFFORTS TO AVOID CARRYING OR PROCESSING ILLEGAL ROBOCALLS

Total Network TEK relies on the methods provided by its upstream provider to measure and combat the transmission or processing of illegal robocalls. They deploy systems to detect potential robocall activity using metrics such as average call duration, Answer Seizure Ratio ("ASR"), and call counts from carrier/consumer reports. Furthermore, Total Network TEK is implementing the following practices to minimize the impact of illegal or unwanted robocalls on our customers:

- **Know Your Upstream Provider:** Knowledge of carriers from which we receive traffic and review whether such carriers are listed in the Robocall Mitigation Database. Total Network TEK has also reviewed each carrier's RMPs to learn how they monitor their originating traffic to mitigate illegal robocalls.
- **Robocall Mitigation Program:** Our upstream provider has in-house software that monitors outbound voice traffic in real time to help prevent the origination of illegal robocalls. Combining behavioral analytics, caller authentication, and verification, the software solution may feature:
 - **FRAUD DETECTION:** Detection of high-volume robocalling, spoofing, and spam call activity.
 - **SUBSCRIBER NOTIFICATION:** Customer Support notifications of suspect activity to warn subscribers of suspicious calls.

- **CALL BLOCKING SUPPORT:** Identification of and enabling end users to block fraudulent phone calls, including using custom and industry available databases for number validation.
- **BUSINESS NUMBER VERIFICATION:** Register legitimate business numbers to prevent unintentional call blocking.
- **CALLER ID NAME SERVICE:** Integration of the Caller ID name lookup service, including robocall mitigation with override to include the original caller ID even when the call is determined fraudulent.
- **CREDIT CARD AND CUSTOMER VALIDATION:** Suspension of fraudulent customers when they match known invalid credit card or other fraud patterns.
- **CONTRACT TERMINATION:** Total Network TEK typically has contractual rights to terminate customers who violate relevant laws, including the Telephone Consumer Protection Act. When appropriate, Total Network TEK enforces these rights. Subject to applicable laws that may prevent it from doing so, Total Network TEK may also terminate accounts if it discovers that any of the entities or individuals associated with a customer account have been named by the Commission or the Federal Trade Commission (“FTC”) as an illegal robocall or have failed to respond to traceback requests.

2.2 TRACEBACK REQUESTS

Total Network TEK commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium.

2.3 COMMITMENT TO COOPERATE IN INVESTIGATING AND STOPPING ILLEGAL ROBOCALLS

Total Network TEK also promptly responds to inquiries from law enforcement and regulators, including the Commission, the FTC, or state attorneys general, seeking traceback or similar information. Total Network TEK commits to continue cooperating with the Commission, law enforcement, and the industry traceback consortium to investigate and stop any illegal robocalls that use Total Network TEK’s services to carry or process calls.

2.4 STIR/SHAKEN COMPLIANCE

Total Network TEK has implemented STIR/SHAKEN for all egress traffic. STIR/SHAKEN uses digital certificates based on common public-key cryptography to ensure the calling number in a telephone call is secure. The expectation is that the certificate technology will enable the called party to verify that the calling number is accurate and that it has not been spoofed.