

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)
FOR
SECOM Inc

Pursuant to 47 C.F.R. § 64.6305, SECOM Inc. submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls ("RMP"). This report describes the status of its implementation of STIR/SHAKEN and the practices and procedures SECOM has in place to mitigate illegal robocalls as of 19 December 2024 (reference RMP below). SECOM may modify, add, delete or otherwise alter any of the policies and procedures described in its RMP at any time in order to respond to changes in its business, its capabilities and its needs.

STIR/SHAKEN Implementation

SECOM commits to fully comply with all conditions set forth in the FCC'S 2020 Report and Order mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission's rules and policies more generally.

SECOM will be implementing STIR/SHAKEN through use of the TransNexus ClearIP software. These are managed end-to-end call authentication solutions that fully satisfy the FCC's STIR/SHAKEN requirements, providing a standardized approach to call authentication and verification (STIR - RFC 8224, RFC 8225, RFC 8226 and SHAKEN- ATIS-1000074-E, ATIS-1000080, ATIS-1000082).

SECOM Inc will be implementing these solutions in the IP portions of its network. A portion of SECOM's traffic relies on technology that cannot initiate, maintain, carry process and terminate SIP calls. Accordingly SECOM is subject to a continuing extension under 47 C.F.R. § 64.6304(d).

- ☐ My traffic is fully attested.
- ☒ My traffic is partially attested.
- ☐ None of my traffic is yet attested, however I have implemented the Robocall Mitigation Plan outlined below.

Robocall Mitigation Plan (updated)

This Robocall Mitigation Plan describes the specific measures that SECOM has implemented to detect and prevent illegal robocalls on its network as of August 25, 2021(updated December 19, 2024). SECOM will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should SECOM determine that changes are appropriate, its practices may differ from those described below.

SECOM has taken the following steps to prevent illegal originating robocalling traffic:

Risk Assessment. SECOM is a voice service provider offering a variety of voice calling services. Its customers generally do not originate high volume calls and SECOM has not received information suggesting that robocalls originate on its network. Therefore, SECOM does not consider its network at high risk of originating illegal robocalls.

Customer Due Diligence: SECOM conducts thorough due diligence on new and renewing customers, confirming the customer's identity and, if a commercial customer, obtains its state of incorporation, its federal tax ID and the general nature of its business. SECOM confirms the physical business location information and service address for all customers.

- SECOM verifies customers' credit history and business reputation prior to providing service.

- SECOM verifies customer information when contracts are renewed, or services are added.
- SECOM verifies customers' identity and their right to use the telephone number presented on calls.
- SECOM has policies in place that define the circumstances by which it will deny, suspend or terminate service to a customer.

SECOM has taken the following steps to prevent or avoid the origination of illegal robocalls:

- SECOM has in place an enforceable terms of service and an acceptable use policy. SECOM also has in place policies designed to detect and prevent fraudulent traffic on its network.
- SECOM uses TransNexus ClearIP analytics technologies and services to monitor traffic on its network and identify potentially unlawful call origination activity. If SECOM reasonably believes that a customer is originating illegal robocalls, it will require the customer to remedy the problem and, if effective action is not taken, service termination may result (as stated in its terms of service).
- SECOM provides its customers with access to call blocking mechanisms and regularly communicates the availability of caller id and call blocking features.

SECOM is a rural telephone services provider and, therefore, has very few trunks connecting its network to upstream providers. SECOM maintains a good relationship with those providers and works with them on a regular basis.

- Due to SECOM's rural location, it is unlikely a new upstream request will be received; however, in the event such occurs, SECOM will consult with the provider to ensure the use of the connection is for legitimate traffic and not for illegal robocalls.
- If SECOM becomes aware that an upstream provider is carrying suspicious traffic, our staff will work with that provider, the FCC and law enforcement to block illegal robocall traffic as soon as possible.

SECOM commits to responding promptly to all trace back requests from the Commission, law enforcement and industry trace back group ("ITG") (the designated official US Traceback Consortium) and to cooperating with such entities in any investigation into illegal robocallers using its service to originate calls.

SECOM will cooperate with state and federal regulators to prevent any and all illegal robocalls and specifically will:

- Respond to valid law enforcement requests;
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and

- Fully implement mandated robocall mitigation procedures with the goal of maximizing the mitigation of illegal robocalls.

This Robocall Mitigation Plan describes the specific measures that SECOM has implemented to detect and prevent illegal robocalls on its network as of August 25, 2021 (and updated as of December 19, 2024). SECOM periodically evaluates the risks it faces, the effectiveness of its policies and procedures and its capabilities to support the measures described. Should SECOM determine that changes are appropriate, its practices may differ from those described above.

SECOM Inc.