



**STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)
FOR
SILVER STAR COMMUNICATIONS (all affiliated companies*)**

Pursuant to 47 C.F.R. § 64.6305, Silver Star Telephone Company, Inc. dba Silver Star Communications ("Silver Star") 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 Silver Star has in place to mitigate illegal robocalls as of February 24, 2024 (reference RMP below). Silver Star 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

Silver Star 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.

Silver Star is implementing STIR/SHAKEN through use of the TNS Call Guardian Authentication Hub and TransNexus 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).

Silver Star has implemented these solutions in the IP portions of its network by February 24, 2024.

- ☐ 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 Silver Star has implemented to detect and prevent illegal robocalls on its network as of June 30, 2021 (updated February 24, 2024). Silver Star will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should Silver Star determine that changes are appropriate, its practices may differ from those described below.

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

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

Customer Due Diligence: Silver Star 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. Silver Star confirms the physical business location information and service address for all customers.

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



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

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

- Silver Star has in place an enforceable terms of service and an acceptable use policy. Silver Star also has in place policies designed to detect and prevent fraudulent traffic on its network.
- Silver Star uses TNS Call Guardian analytics technologies and services to monitor traffic on its network and identify potentially unlawful call origination activity. If Silver Star 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).
- Silver Star's wireless services utilize TransNexus software to maintain STIR/SHAKEN compliance for wireless voice traffic.
- Silver Star provides its customers with access to call blocking mechanisms and regularly communicates the availability of caller id and call blocking features.
- Silver Stars robocall mitigation policies are publicly available on its website.

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

- Due to Silver Star's rural location, it is unlikely a new upstream request will be received; however, in the event such occurs, Silver Star will consult with the provider to ensure the use of the connection is for legitimate traffic and not for illegal robocalls.
- If Silver Star 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.

Silver Star 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.

- Silver Star has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual. It either has provided the ITG with the contact information and business hours for those individuals or will do so upon receipt of the first request from the ITG. See <https://www.ustelecom.org/the-industry-traceback-group-itg/for-providers/>.

Silver Star 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



- Implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.

Silver Star certifies that it (*including affiliates listed below) is not, nor has it, been prohibited from filing in the Robocall Mitigation Database and has not, at any time in the prior two years, been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing relating to claims of transmitting, encouraging, assisting or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

This Robocall Mitigation Plan describes the specific measures that Silver Star has implemented to detect and prevent illegal robocalls on its network as of June 30, 2021 (and updated as of February 24, 2024). Silver Star periodically evaluates the risks it faces, the effectiveness of its policies and procedures and its capabilities to support the measures described. Should Silver Star determine that changes are appropriate, its practices may differ from those described above.

*** Columbine Telephone Company, Inc.
Gold Star Communications, LLC
Millennium Networks, LLC
Silver Star Telephone Company, Inc.**