

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, Chariton Valley Broadband, LLC (the “Company”) submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This report describes the status of STIR/SHAKEN implementation and the Company's practices and procedures to mitigate illegal robocalls as of June 30, 2021. The Company may modify, add, delete, or otherwise alter any of the policies and procedures described in the plan at any time to respond to changes in its business, capabilities, and needs.

STIR/SHAKEN Implementation

The Company will comply fully 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.

The Company is implementing STIR/SHAKEN using the TNS Call Guardian Authentication Hub. This is a managed end-to-end call authentication solution that fully satisfies the FCC’s STIR/SHAKEN requirements. It provides a standardized approach to call authentication and verification (STIR – RFC 8224, RFC 8225, RFC 8226, and SHAKEN – ATIS-1000074-E, ATIS-1000080, ATIS-1000082).

The Company will implement this solution by the applicable deadline. The Company is subject to the small-voice-provider STIR/SHAKEN extension under 47 C.F.R. §64.6304(a) because it is a provider with 100,000 or fewer voice service subscriber lines. The Company has implemented the Robocall Mitigation Plan outlined below.

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that the Company has implemented to detect and prevent illegal robocalls on its network as of June 30, 2021. The Company will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should the company determine that changes are appropriate, its practices may differ from those described below.

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

SPECIFIC MEASURES TO IDENTIFY AND PREVENT ILLEGAL ROBOCALLS

Know Your Customer: The Company conducts due diligence on new and renewing customers, confirming that each customer is a business and that its formation documents are in order. The Company confirms the customer’s service address for all customers.

- The Company verifies the customer's credit history and business reputation prior to providing service.
- The Company verifies customer information when contracts are renewed or services are added.
- The Company verifies the customer's identity and their right to use the telephone number presented on calls.
- The Company has policies that define the circumstances under which it will deny, suspend, or terminate service to a customer.

Know Your Upstream Provider: The Company has a vetting and review process for all upstream providers that send us voice traffic and that we terminate or transit to other providers. Before accepting traffic, we verify that each upstream provider is properly registered in the FCC's Robocall Mitigation Database, has an authorized STIR/SHAKEN implementation status, and has published a valid robocall mitigation plan, including a vetting process for their customers and upstream providers and the appropriate means to identify suspicious traffic. We will not accept voice traffic from an unregistered provider.

The company maintains a clear understanding of the identity, legitimacy, and compliance posture of all upstream providers from whom we receive traffic, which includes an understanding of the upstream provider's role in the call path for the traffic they will send us, specifically identifying whether they are acting as an originating voice service provider, a foreign intermediate provider, or a U.S.-based intermediate provider.

Our contractual provisions with upstream providers prohibit them from sending us any illegal traffic. If we find that an upstream provider is sending us suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

We conduct ongoing monitoring to ensure that upstream partners adhere to industry standards and FCC requirements, including reviewing their mitigation practices, monitoring traffic patterns for anomalies, and taking corrective action when necessary. These measures help ensure that we accept traffic only from trusted, compliant sources and reduce the risk of unlawful robocalls entering our network.

Measures to Prevent or Avoid the Origination of Illegal Robocalls

- The Company has in place enforceable terms of use and/or an acceptable use policy. The Company also has in place policies designed to detect and prevent fraudulent traffic on its network.
- The Company uses TNS Call Guardian analytics technologies and services to monitor traffic on its network and identify potentially unlawful call origination activity. If the

Company has a reasonable basis to believe that a customer is originating illegal robocalls, the Company will investigate and will require the customer to remedy the problem. If effective action is not taken, the Company can suspend and/or terminate service to the customer.

- The Company blocks the following types of calls by default:
 - ☒ Calls originating from invalid numbers per FCC Order **[2017 Call Blocking Order]**
 - ☒ Calls from DNO numbers as per FCC Order **[2017 Call Blocking Order]**
- The Company also blocks the following types of calls:
 - Known blacklisted IP addresses are monitored and blocked on a regular basis
 - Calls to the PSTN are monitored with call blocking management, which sets non-domestic trunk limits to halt fraudulent calls.
 - Call appearances are limited to the PSTN to values necessary for valid calling patterns
 - Trunk usage alarms and notifies of high usage values if thresholds are exceeded.

Responding to Traceback Requests

- The Company will respond within 24 hours to all traceback requests received from the Commission, law enforcement, and the Industry Traceback Group (ITG). If a pattern of questionable activity is detected, The Company will require its customer to remedy the problem and, if effective action is not taken, may suspend and/or terminate service to the customer.
- The Company has designated an individual as a dedicated point of contact for addressing traceback requests and a backup for that individual. It has either provided the ITG with the contact information and business hours for those individuals, or will do so upon receipt of the ITG's first request. See <https://www.ustelecom.org/the-industry-traceback-group-itg/for-providers/>
- The Company will cooperate with the Commission, state regulators, law enforcement, and the ITG to investigate and prevent illegal robocalls. Among other things, the Company 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.

The Company has deployed TNS-provided call authentication, call labeling, and call blocking services. We have made great strides to protect our networks and consumers from harmful calls. The Company is pleased to play a role in that improvement and will continue the necessary work to protect our customers.