

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, **Blackfoot Telephone Cooperative, Inc.. DBA Blackfoot Communications (“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 its implementation of STIR/SHAKEN and the practices and procedures **Company** has in place to mitigate illegal robocalls as of June 30, 2021. **Company** may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time in order to respond to changes in its business, its capabilities and its needs.

STIR/SHAKEN Implementation

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.

Company is implementing STIR/SHAKEN through use of 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).

[**Company**] expects to implement this solution in the IP portions of its network by June 30, 2021.

- ☐ 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

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

SPECIFIC MEASURES TO IDENTIFY AND PREVENT ILLEGAL ROBOCALLS

Customer Due Diligence: **Company** conducts due diligence on new and renewing customers, confirming the customer's identity and, if it is a business, its incorporation documents. The **Company** confirms the customer's service address for all customers.

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

Measures to Prevent or Avoid the Origination of Illegal Robocalls

- **Company** has in place an enforceable terms of use and/or an acceptable use policy. **Company** also has in place policies designed to detect and prevent fraudulent traffic on its network.
- **Company** uses TNS Call Guardian analytics technologies and services to monitor traffic on its network and identify potentially unlawful call origination activity. If **Company** has a reasonable basis to believe that a customer is originating illegal robocalls, it will require the customer to remedy the problem and, if effective action is not taken, **Company** can suspend and/or terminate service to the customer.
- **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]**
- **[Company]** also blocks the following types of calls:
 - ✓ Describe any blocking based on FCC safe harbors – analytics, network-based blocking, etc.
 - ✓ Describe any other blocking policies.

Responding to Traceback Requests

- **Company** 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/>
- **Company** will respond promptly to inquiries received from the Industry Traceback Group. If a pattern of questionable activity is detected, **Company** will require its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated.

Cooperation with State and Federal Regulators

Company will cooperate with state and federal regulators to prevent any and all illegal robocalls. Specifically, **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.

Company has deployed call authentication, call labeling, and call blocking services provided by TNS. We have made great strides to protect our networks and consumers from harmful calls.

Company is pleased to play a role in that improvement and will continue the necessary work to protect our customers.

Sincerely,
/s/ **JB Ray**