



February 20, 2024

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, DirectLink 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 DirectLink has in place to mitigate illegal robocalls as of February 20, 2024. DirectLink 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, its capabilities, and its needs.

STIR/SHAKEN Implementation

DirectLink has fully implemented STIR/SHAKEN through use of the Trans Nexus Clear IP. 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).

All the voice traffic that originates on our network is subject to the robocall mitigation program described 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. 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. DirectLink is a voice service provider offering a variety of voicecalling services. Its customers generally do not originate high volume calls and DirectLink has not received information suggesting that robocalls are originated on its network. Therefore, DirectLink does not consider its network at high risk of originating illegal robocalls.

SPECIFIC MEASURES TO IDENTIFY AND PREVENT ILLEGAL ROBOCALLS

Know your Customer. We follow the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

This process includes the collection and review of entity-identifying information to confirm that we have an authenticated relationship with the customer. We use this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

We also validate, when possible, that the entity has a legitimate right to use its asserted calling numbers. We use this information to support the attestation level we assign to calls that we originate for that customer.

Our contractual provisions with customers prohibit them from initiating illegal robocalls. If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

Customer Due Diligence: DirectLink 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.

- DirectLink verifies customer's credit history and business reputation prior to providing service.
- DirectLink verifies customer information when contracts are renewed, or services are added.
- DirectLink verifies the customer's identity and their right to use the telephone number presented on calls.
- DirectLink 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

- DirectLink has in place policies designed to detect and prevent fraudulent traffic on its network.
- We use software provided by TransNexus to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls. The software provides detailed reporting identifying suspected illegal robocalls and alerts us if we originate any calls where the calling number is invalid, unallocated, on a Do Not Originate list, in the FCC consumer complaint database or has a poor reputation. We immediately investigate any identified calls to determine if the caller was attempting to originate unlawful robocalls. If we determine that the caller was attempting to originate unlawful robocalls, then we either warn them to stop or terminate their service as appropriate.

Upstream Providers

We establish an understanding of the upstream provider's role in the call path for the traffic they will send to us, for example, whether they are acting as an originating voice service provider, a foreign intermediate provider, or a U.S.-based intermediate provider. We use this information to understand whether we will be obligated to authenticate unsigned traffic that we receive from them.

Our contractual provisions with upstream providers prohibit them from sending us illegal robocalls. 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.

Responding to Traceback Requests

- We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls.
- DirectLink has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual. It will



provide the Industry Traceback group (ITG) with the contact information and business hours for those individuals.

Dedicated Point of Contact for Industry Traceback Group.

Erik Kehler

Director Of Plant and Field Operations

Email: eric.kehler@cbsoregon.com

503.266.8223

8am to 5pm PST

- DirectLink will respond within 24 hours to inquiries received from the Industry Traceback Group. If a pattern of questionable activity is detected, DirectLink 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

DirectLink will cooperate with state and federal regulators to prevent all illegal robocalls. Specifically, DirectLink 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 possible with the goal of maximizing the mitigation of illegal robocalls.

Sincerely,

Paul E Hauer
President/CEO
503-266-8200