

ROBOCALL MITIGATION PLAN

This document describes the steps that Centre WISP Venture Company, LLC d/b/a Black Bear Fiber (Centre WISP) is taking to meet the revised Robocall Mitigation Database filing requirements and related rules adopted in the Federal Communications Commission's ("FCC") *Sixth Caller ID Authentication Report and Order*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18 (rel. Mar. 17, 2023).

Pursuant to 47 CFR § 64.6305, this Robocall Mitigation Plan describes the specific steps we are taking to avoid the origination, carrying, or processing of illegal robocall traffic. We will periodically evaluate the risks we face, the effectiveness of our policies and procedures, and our capabilities to support the measures described. Should we determine that changes are appropriate, we may alter our practices from those described below. We 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 our business, capabilities and needs.

I. Filer Information

Centre WISP is an internet service provider. We are currently deploying infrastructure to offer voice and broadband services to customers within the general area of rural central pennsylvania, and are launching the commercial offering of service.

II. STIR/SHAKEN Certification

Pursuant to 47 CFR § 64.6304(b), Centre WISP Venture Company, LLC is exempt from the FCC's caller ID authentication requirements because it lacks control over the network infrastructure necessary to implement STIR/SHAKEN. We provide voice service to our end-user customers by reselling voice service provisioned using the Telnyx, LLC (FRN 0018998724) wholesale voice platform. Telnyx has certified in the FCC's Robocall Mitigation Database that it has implemented STIR/SHAKEN. Telnyx, LLC. is listed as an authorized provider on the Secure Telephone Identify Policy Administrator list. Centre WISP Venture Company, LLC hereby certifies that it is a voice provider not subject to a STIR/SHAKEN implementation obligation.

III. Know-Your-Upstream Providers Procedures

Centre WISP incorporates by reference the measures implemented by Telnyx to know its upstream providers, as reflected in Telnyx's Robocall Mitigation Plan.

IV. Know-Your-Customer Procedures

The vast majority of our end user customers are either residential or single-party business lines. These customers are limited to one call path, thereby minimizing the overall risk of robocalls originating from our customers. We have not received information suggesting that robocalls are likely to originate on our network. Therefore, we do not consider our network at high risk of originating illegal robocalls.

As a locally-based company, we know our customers – our customers are members of the local community we operate in.

As part of our standard operating procedure, we will be conducting due diligence on new and renewing voice customers, confirming the customer's identity and whether it is a business. For business customers, we will confirm:

- Contact person
- Physical business location
- State incorporation
- Federal tax ID
- Nature of the business

V. Contractual Terms and Other Measures

We have in place an enforceable terms of service/acceptable use policy that prohibits our customers from engaging in robocalling.

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

Our customers are not allowed to self-provision voice services using their broadband connection. We only sell voice services to physical locations that are on our network. The provisioning information connecting our voice customers to the PSTN via VoIP is provisioned directly by the service provider and cannot be moved or altered by an end user customer.

VI. Fraud Detection and Analytics

Telnyx collects contact and company information for each new customer upon sign-up. In line with our AUP and Terms and Conditions, Telnyx can leverage such contact information when we detect fraudulent call patterns to notify the customer of potential blocking or to pass such contact information to traceback administrators or law enforcement agents when necessary.

Telnyx takes the following steps to minimize the risk of fraud originating on our network. First, Telnyx blocks any subscribers who attempt to sign up with a “free-mail” account to reduce the risk of inviting bad actors onto our platform. Upon signing up with a valid e-mail, Telnyx customers are significantly limited to the amount of traffic they can originate from our platform. Suppose the customer wishes to increase their origination thresholds. In that case, they can apply for “level 2 verification,” which includes a more in-depth review of the company's calling patterns, business model, and any previous complaints. Telnyx monitors traffic patterns, primarily tracking answer success rates (“ASR”) and average call duration (“ACD”), by all new and existing customers and immediately takes steps to block the account if the patterns mentioned above reflect fraudulent activity. In addition to internal monitoring tools, we have implemented a third-party analytics provider (Nomorobo) that monitors traffic patterns through machine learning to alert our fraud team of suspicious activity or calling patterns. Telnyx currently blocks any originating call with an invalid ANI and is in the process of implementing

the US Telecom DNO list to ensure we catch any potential fraudulent call from leaving our platform. In addition to calling patterns, Telnix has implemented payment method tracking to block any customer with suspicious payment activities.

VII. Enforcement

We commit to respond to respond within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use our service to carry or process calls.

We have designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual. We will provide the Industry Traceback Group (ITG) with the contact information and business hours for those individuals upon receipt of the first request from the ITG. See

<https://www.ustelecom.org/the-industry-traceback-group-itg/for-providers/>

If a pattern of questionable activity is detected, we will require our customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated.

VIII. Cooperation with State and Federal Regulators

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

IX. Additional Certifications

We hereby certify that we have not been prohibited from filing in the Robocall Mitigation Database.

In the prior two years, we have not been subject to an FCC, law enforcement or regulatory agency action or investigation due to alleged robocalling, or spoofing.



David Gibbons, CEO

2025/09/18

Date