

ROBOCALL MITIGATION PLAN

This document describes the steps that the City of Longmont, a Colorado municipal corporation acting on behalf of its Electric and Broadband Utility Enterprise (NextLight) 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

The City of Longmont is a municipal corporation located in the state of Colorado. Acting on behalf of its Electric and Broadband Utility Enterprise (NextLight) has developed and established broadband service offerings including Internet access services and VoIP Phone services delivered via a fiber to the unit architecture to residents living in the City of Longmont, Colorado.

II. STIR/SHAKEN Certification

NextLight hereby certifies that all voice traffic originating on its network is authenticated in compliance with the applicable standards under 47 CFR § 64.6301. We provide voice service to our end-user customers by reselling voice service provisioned using the Alianza wholesale voice platform. Alianza has certified in the FCC's Robocall Mitigation Database that it has implemented STIR/SHAKEN. Alianza, Inc. is listed as an authorized provider on the Secure Telephone Identify Policy Administrator list.

III. Know-Your-Upstream Providers Procedures

NextLight incorporates by reference the measures implemented by Alianza to know its upstream providers, as reflected in Alianza's Robocall Mitigation Plan. In particular, Alianza has existing agreements with Tier-1 carrier service providers from which it facilitates the provision of service to its service provider customers. Alianza has confirmed that each of those carriers are listed in the Robocall Mitigation Database.

IV. Know-Your-Customer Procedures

The City of Longmont is a municipal corporation acting on behalf of its Electric and Broadband Utility Enterprise (NextLight), offering voice calling services and broadband to end user customers. Our customers are located within the City of Longmont and are all customers of the electric cooperative. As such, we know our customers – our customers are apart of the community we operate in, and customers of the electric utility. 2 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 part of our standard operating procedure, we conduct due diligence on new and renewing voice customers, confirming the customer's identity and whether it is a business. For business customers, we 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.

Alianza's contractual agreements with its underlying carrier service providers also include provisions requiring the parties' compliance with applicable robocall prevention and mitigation standards.

VI. Fraud Detection and Analytics

Our wholesale provider, Alianza, has implemented a proprietary fraud detection and mitigation process through which it analyzes high-volume network traffic to evaluate compliance with a variety of fraud detection indicators and fraud detection best practices. Through this fraud detection and mitigation process, Alianza will notify individual customers (i.e. NextLight) of potentially fraudulent activity occurring in any of that customer's subscriber accounts. Alianza may take remedial action against any subscriber's account to prevent or remediate robocalling or other fraudulent activity. If Alianza takes any such action, its fraud detection system triggers notification to the customer of that action and any remedial steps that may be taken to restore service.

VII. Enforcement

We commit 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/forproviders/>

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.

[Name/title of certifying official]

[date]