

NORTHWEST OPEN ACCESS NETWORK ROBOCALL MITIGATION PLAN

As part of NoaNet's submission to the Robocall Mitigation Database, pursuant to the FCC's *Sixth Caller ID Authentication Report and Order*, and applicable predecessor orders, this document describes (1) the specific reasonable steps NoaNet takes to avoid carrying illegal robocall traffic; (2) NoaNet's commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium; and (3) NoaNet's commitment to cooperate with such entities in investigating and stopping any illegal robocallers that use the provider's service to carry or process calls.²

I. CORPORATE INFORMATION

- NoaNet certifies it has not been prohibited from filing in the Robocall Mitigation Database and NoaNet has not been subject to any Commission, law enforcement, or regulatory agency action or investigation arising from suspected unlawful robocalling or spoofing.
- In accordance with 47 CFR 64.6305(c), NoaNet has designated a point of contact to receive notice of any issues. The contact person's information is available within the Robocall Mitigation Database.

² See *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18 (Mar. 17, 2023). See also *Wireline Competition Bureau Announces Robocall Mitigation Database Filing Deadlines and Instructions and Additional Compliance Dates*, Public Notice, WC Docket No. 17-97 (Jan. 25, 2024).

II. DESCRIPTION OF ROBOCALL MITIGATION PROGRAM

A. Efforts to Avoid Carrying Illegal Robocalls

NoaNet does not operate any VOIP or SIP originating or terminating equipment. All calls would only traverse, the network and are subject to a robocall mitigation program reasonably expected to help reduce the origination, processing or carrying of illegal robocalls. NoaNet provides the following solutions on the NoaNet network to help minimize the impact of illegal or unwanted robocalls on customers:

- **Know Your Customer/Know Your Upstream Provider:** NoaNet has a “Know Your Customer Team” comprised of multiple employees. This team conducts “know your customer” and “know your upstream provider” vetting before it allows a party to become a new customer. Among other tests, the team will investigate the type of service being sought by the prospective customer and review the potential customer’s website to ensure that it has functional links and is not using fictitious names. NoaNet’s Know Your Customer team will research whether the prospective customer is located overseas, we do not provide service to overseas customers, (which would require meeting of Know Your Upstream Provider), and whether the FCC or the FTC have sent the prospective customer of individuals associated with the customer letters identifying them as involved in robocalling or spoofing. Additionally, NoaNet’s Know Your Customer team will ensure that a prospective customer is registered in the FCC’s robocall mitigation database (and does not withdraw such registration) if the customer is classified by the FCC as a “provider.” Any information that is provided to NoaNet is compared to public information available either on the customer’s website or through other internet-based resources.
- **Teaming with Others:** NoaNet works with other companies to stop unlawful robocalls. For example, NoaNet has worked with “GoTo.” GoTo alerts if there is unusual usage on certain numbers. NoaNet then contacts the customer to investigate and to take potential action.
- **Contract Termination:** NoaNet typically has contractual rights that allow it to terminate customers that violate any relevant law and to immediately suspend service to protect the network, including violations of the Telephone Consumer Protection Act. When appropriate, NoaNet enforces these rights. Subject to applicable laws that may prevent it from doing so, NoaNet may also terminate accounts if it discovers that any of the entities or individuals associated with a customer account have been named by the FCC or the FTC as an illegal robocaller or have failed to respond to traceback requests.

As a rural wholesale ISP which only resells VOIP service but does not provide any originating or terminating SIP sessions, NoaNet does not have a direct relationship with a party that maybe originating unlawful robocalls. Accordingly, when NoaNet suspects it has identified unlawful calling, in addition to taking the steps identified above, it may also contact the party sending NoaNet the calls (i.e., NoaNet's carrier/provider customer), and request that they work to investigate their customers (e.g., to identify the party sending them the calls, determine whether the calls are unlawful, and then to eliminate the source of the calling).

B. Traceback Requests

The Industry Traceback Group ("ITG") is a collaborative effort of companies across the wireline, wireless, VoIP and cable industries that actively trace and identify the source of illegal robocalls. The Robocall Strike Force was created to accelerate the development and adoption of new tools and solutions to abate the proliferation of illegal and unwanted robocalls, to promote greater consumer control over the calls they wish to receive, and to make recommendations to the FCC. NoaNet commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium.

C. Commitment to Cooperate in Investigating and Stopping Illegal Robocallers

NoaNet also promptly responds to inquiries from law enforcement and regulators, including the FCC, Federal Trade Commission (“FTC”) or state attorneys general seeking traceback or similar information. NoaNet commits to cooperate with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that use NoaNet’s services to carry or process calls.

D. STIR/SHAKEN Compliance

Although its role as a wholesale provider and reseller is somewhat unique and is exempt from STIR/SHAKEN Compliance, NoaNet has ensured that all SIP headers which transit the network pass through any authentication information unaltered. Additionally, NoaNet has worked actively with Comcast, Inteliquent and T-Mobile to test SIP call delivery for Public Safety and 911 calls across their implemented STIR/SHAKEN networks to ensure PSAP calls are delivered correctly.

NoaNet uses Alianza as a provider and analytics provider with Metaswitch.