

DECLARATION NETWORKS GROUP, INC.

ROBOCALL MITIGATION PLAN

Declaration Networks Group, Inc. d/b/a Neubeam, Sound Internet Services, and PogoZone (“DNG” or “Company”) is a provider of broadband services in rural areas, providing both fixed wireless and fiber internet services and VoIP provider with a STIR/SHAKEN implementation obligation serving end-users in the states of Washington, Virginia and Maryland. DNG provides some of its services by reselling the VoIP services of Momentum Telecom, Inc. DNG has also implemented the ClearIP monitoring system from TransNexus to implement STIR/SHAKEN for the VoIP services provided directly to its customers. DNG’s OCN number is 260K.

Certification

Company, by submitting this RMP, hereby certifies that (a) all calls originating on its network are subject to this RMP which satisfies the FCC’s requirements, (b) any prior certification of the Company has not been removed by Commission action and (c) DNG (including any parent and affiliates) has not been prohibited from filing in the Robocall Mitigation Database (“RMD”) by the Commission. The Company has also certified that it has fully implemented STIR/SHAKEN across its own network and all calls it originates are compliant with Commission rules. DNG (and any parent, affiliate or any entity that shares common ownership, management, directors, or control) has not been the subject of any formal Commission law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient RMD certification or RMP description.

Know-Your Customer Policies

Wholesale Services:

DNG prohibits the resale of our VoIP services.

Retail Services:

A sales representative collects all contact information, and a physical installation by a technician is required, thereby confirming the location and type of business or residence. Each customer signs a contract that includes our terms of service.

For Services provided directly by DNG, Pogo has partnered with TransNexus to optimize our efforts in monitoring our outbound voice traffic in real-time to prevent the origination of illegal robocalls. TransNexus is a leading provider of cloud-ready, high-performance, scalable software-based VoIP and WebRTC session control infrastructure. The TransNexus ClearIP monitoring system software provides detailed reporting, identifies 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 been flagged for 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.

As part of the vetting process, DNG collects information such as physical location, contact person(s), and for small businesses, the nature of the customer's business, among other things. Doing so is necessary to provide a prompt response to traceback requests and enforcement efforts.

With these measures and procedures along with those discussed herein, below, Pogo takes "affirmative, effective measures to (1) prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic" and (2) know its upstream providers.

Through its retail terms of service, DNG requires customers to comply with all applicable laws in relation to its voice services, explicitly prohibiting any abusive or unlawful use of the service. Below are applicable excerpts:

2.4 Prohibited Uses.

(a) Unlawful. You shall use the Service and the Device only for lawful purposes. We reserve the right to immediately disconnect your Service without notice, if, in our sole and absolute discretion, we determine that you have used the Service or the Device for an unlawful purpose. In the event of such disconnection, you will be responsible for the full month's charges to the end of the current term, including, without limitation, unbilled charges, plus a disconnection fee, if applicable, all of which will become immediately due and payable upon disconnection of your Service. If we believe that you have used the Service or the Device for an unlawful purpose, we may forward the relevant communication and other information, including your identity, to the appropriate authorities for investigation and prosecution. You hereby consent to our forwarding of any such communications and information to these authorities. In addition, DNG will provide information in response to law enforcement requests, lawful government requests, subpoenas, court orders, to protect its rights and property and in the case where failure to disclose the information may lead to imminent harm to the customer or others.

(b) Inappropriate Conduct. You shall not use the Service or the Device in any way that is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy, or any similar behavior. We reserve the right to immediately disconnect your Service without notice, if, in our sole and absolute discretion, we determine that you have used the Service or the Device in any of the aforementioned ways. In the event of such disconnection, you will be responsible for the full month's charges to the end of the current term, including, without limitation, unbilled charges, plus a disconnection fee, if applicable, all of which will become immediately due and payable upon disconnection of your Service. If we believe that you have used the Service or the Device in any of the aforementioned ways, we may forward the relevant communication and other information, including your identity, to the appropriate authorities for investigation and prosecution. You hereby consent to our forwarding of any such communications and information to these authorities. In addition, DNG will provide information in response to law enforcement requests, subpoenas, court orders, to protect its rights and property and in the case where failure to disclose the information may lead to imminent harm to the customer or others. Furthermore, DNG reserves all of its rights at law and equity to proceed against anyone who uses the Services illegally or improperly.

2.4.1 Additional Prohibited Uses. Permitted use of the Service does not include certain activities including, but not limited to autodialing, robocalling, transmitting any

material that contains viruses, time bombs, trojan horses, worms, malware, spyware, or any other programs that may be harmful or dangerous, spoofing, continuous or extensive call forwarding, continuous connectivity, fax broadcast, fax blasting, polling, transmitting any material that may infringe, misappropriate, or otherwise violate the foreign or domestic intellectual property rights or other rights of third parties, telemarketing (including without limitation charitable or political solicitation, junk faxing, fax spamming, calling/faxing any person through the use of distribution lists or otherwise who has not given specific permission to be included in such a process) or any other activity that would be inconsistent with reasonable business usage.

You further agree not to transmit any material that encourages conduct that could constitute a criminal offense, violate the intellectual property rights of others, give rise to civil or criminal liability or otherwise violate any applicable local, state, national or international statute, regulation, or other law. You agree that you will, at all times, comply with all applicable law. You hereby acknowledge and agree to abide by the terms of the FCC's Declaratory Ruling (CG Docket No. 23-362) dated February 8, 2024 whereby the FCC clarified that calls made with AI-generated voices are "artificial" under the Telephone Consumer Protection Act ("TCPA") which means that voice cloning technology used in common robocall scams targeting consumers illegal. Applicable law includes, as applicable, the Telephone Consumer Protection Act and the Telemarketing Sales Rule, the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act ("TRACED Act"), the Truth in Caller ID Act, the Junk Fax Act, the CAN-SPAM Act, similar state laws, state laws regarding privacy and data subject rights, and the requirements of the Payment Card Industry Data Security Standard ("PCI DSS"). You agree that the Services are not intended for use with alarm systems or elevator telephone systems.

2.13 Resale.

Company's Services are not intended to be resold by third parties. Customer shall not resell the Company's Services in whole or in part without the Company's express written consent which may withheld at Company's discretion. In the event that resale is permitted and Customer purchases Service(s) for resale, Customer shall be solely responsible for the interaction between Customer and Customer's end users with respect to the Services. Customer will cooperate with Company to enable Company to provide the Services and will allow Company to use any customer proprietary network information (information that relates to the quantity, technical configuration, type, destination and amount of use of the Services by an end user and that is made available to Company as a result of Company's provision of the Services) from such end users to facilitate the provision of Service and to offer additional services to such users. Customer's authorization to Company to use, disclose and permit access to customer proprietary network information will remain in effect until Customer affirmatively terminates such access. The following terms and conditions shall apply to Customer's rights and responsibilities as an authorized reseller of the Services:

(1) Customer is solely responsible for obtaining all licenses, approvals, and regulatory authority for its use and operation of the Services and the provision of Services to its end users. In connection with its resale of the Services, Customer is solely responsible for all billing, billing adjustments/credits, customer service, creditworthiness and other service-related requirements of its end users, and Company shall have no liability to Customer's end users. Customer's payment obligations hereunder are not contingent upon Customer's ability to collect payments or charges from its end users or any other third party. In addition to the remedies for failure of

Customer to make payment set out elsewhere (including in these Terms and Conditions), if Customer fails to make payment for the underlying Service that is being resold to a third party then Company reserves the right to directly bill the end user customer for the Service at Company's sole discretion.

(2) Company may, without penalty, suspend any or all of the Services immediately and/or terminate Contract and/or Service Order(s) with Customer then in place if: (a) Customer fails to comply with any applicable foreign, federal, state or local law or regulation applicable to Customer's resale of the Services; (b) Customer or its end user(s) commit any illegal acts relating to or involving the Services; or (c) Customer uses the Services in a manner which, in the opinion of Company, are illicit or improper. During any period of suspension pursuant to the foregoing sentence, no Service outage or interruption shall be deemed to occur. Customer shall: (i) be liable to Company for any damages caused by any acts of Customer or its end users, in connection with its use or resale of the Services; and (ii) indemnify, defend and hold Company, its Affiliates, agents, and contractors harmless from and against any third party (including end users') claims, actions, damages, liabilities, costs, judgments or expenses (including attorney fees) arising out of or relating to Customer's or end user's use, resale or modification of the Services or Customer's failure to comply with any regulatory filing or reporting requirements or failure to make any required regulatory or contributory payments (including but not limited to universal service support mechanisms).

(3) Customer shall not be excused from paying for Services on the basis that fraudulent calls, unauthorized use or other usage of the Service comprised a portion (or all) of Customer's utilization of the Service. Customer shall protect, defend, indemnify, and hold harmless Company, its officers, directors, employees, contractors, and agents, from and against any and all liabilities, allegations, claims, losses, damages, expenses (including reasonable attorney's fees and costs), judgments, and causes of action arising from or related to fraudulent calls, unauthorized use or usage of the Service to the extent that the person or entity claiming the calls or usage to be fraudulent is (or had been at the time of the call or usage) a user or other person or entity that would have had access to the Service through Customer. Company shall be entitled to take immediate action without notice or liability to Customer as it deems necessary in its sole discretion to prevent fraudulent calls or other usage of the Service; provided, however, that Company is under no obligation to undertake such action.

(4) Robocalling Mitigation Database Registration. If Customer is considered a domestic or foreign voice service provider by the FCC, Customer is required to register with the FCC's [Robocall Mitigation Database](#). As mandated by the FCC, Company will block or otherwise not transmit Customer's voice calls to or from a United States phone number if Customer is not registered in the FCC's [Robocall Mitigation Database](#).

To the extent a customer is found to have violated its contractual obligations for the reasons noted previously or any other reason, DNG will take action commensurate with the severity of the customer's offense, including, but not limited to, providing the customer with a warning or terminating the customer's service and/or reporting the misconduct to the appropriate authorities.

Use of Call Analytics to Identify and Block Unlawful Traffic

For certain customers, DNG utilizes Momentum as a third-party provider of VoIP services, therefore DNG relies on procedures, policies, and safeguards implemented by Momentum to

ensure that its residential and business customers are sufficiently protected against robocall and spoofing activities. Momentum has implemented STIR/SHAKEN within its network and signs the originating calls on behalf of DNG's customers. Momentum utilizes the Sansay and TransNexus STIR/SHAKEN platforms. For its remaining VoIP customers, DNG has fully implementing the ClearIP monitoring system from TransNexus to implement STIR/SHAKEN for the VoIP services provided directly to its customers.

As a reseller of Momentum's VoIP service, DNG uses Momentum's systems for porting phone numbers and provisioning services to our customers. They have complete visibility into our customer information and traffic, and we rely on their network monitoring to initially identify potential robocallers. We work closely with them when potential illegal activity is identified per their Robocall Mitigation Plan:

In the event that Momentum's analytics report indicates potential illegal robocall activity by a wholesale end user customer, Momentum alerts the wholesale customer's contact representative and asks the customer to investigate the issue and thereafter inform Momentum: (i) when the issue is resolved and (ii) what actions the wholesale customer took in resolving the issue.

Knowledge of Upstream Providers

DNG follows the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>). DNG's Know Your Upstream Provider procedure involves checking the RMD to see if the Provider's filing (a) appropriately appears in the RMD, (b) shows that the provider has submitted the applicable filing, and (c) has not been de-listed pursuant to an enforcement action. Momentum serves as DNG's sole Intermediate Provider, which are currently and appropriately listed in the RMD, and DNG does not directly connect to any other provider.

Momentum knows all of the upstream providers from which it directly receives traffic and has insight into its upstream providers' policies and procedures related to identifying and blocking unlawful robocall traffic through Momentum's review of these providers' robocall mitigation plans. Momentum confirms that all upstream providers from which it receives traffic are listed in the FCC's Robocall Mitigation Database.

Cooperation with the Traceback Group, Law Enforcement and Government Agencies

DNG is committed to responding fully and within 24 hours to all traceback requests made by ITG, law enforcement authorities, and government agencies to investigate and address suspected unlawful robocalls originated or passed to DNG customers.

DNG is committed to fully complying with the Commission's robocall blocking requirements and confirms that it will work with Momentum to block all calls and provider traffic that: (1) are identified in any public notice or order released by the FCC; (2) are substantially similar to the types of traffic identified in any public notice or order released by the Commission; or (3) include a caller ID number or name that is on DNO list issued by ITG. Momentum also blocks the traffic of all foreign providers and gateway providers that have not registered in the Robocall Mitigation Database.

Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues

To further ensure DNG's network is not utilized for the origination, termination, or carrying or processing of unwanted and illegal robocalls, DNG provides the following name, title, department, business address, telephone number, and email address of the individual within DNG that leads DNG's team that handles robocall mitigation-related issues as well as responds to traceback inquiries from the FCC, ITG, and law enforcement agencies:

Contact Name: Warren Brasselle
Contact Title: VP Network Operations
Contact Department: Main Office
Contact Street Address: 8245 Boone Boulevard, Suite 230
Contact City State and Zip Code: Vienna, VA 22182
Contact Telephone Number: (703) 282-4385
Contact Email: Warren@declarationnetworks.com

Updates to DNG's RMD Submission and RMP

The Company agrees to update its submission in the RMD within ten (10) business days of any change to the applicable information it must provide and update in the RMD.