

PUREVOIP LLC ROBOCALL MITIGATION PLAN

I. PUREVOIP's Know Your Customer ("KYC") Standards

PUREVOIP is a wholesale, intermediate provider that focuses its business and operations on the wholesale voice services communications market. As part of its customer-onboarding process, PUREVOIP undertakes various commercially reasonable precautions to verify a given customer's identity, including having its customers complete a KYC questionnaire, a USF Exemption Certificate, and a formal written contract. Among other data points collected and, as appropriate, verified, as part of those processes PUREVOIP gathers the following customer identifying facts and circumstances:

- Customer business name,
- state or country of incorporation,
- physical business location,
- contact person(s), with business phone number and email address;
- federal tax ID number,
- FCC Filer ID;
- Robocall Mitigation Database filing indicating STIR/SHAKEN compliance; and
- Company website and/or other customer-facing presence;

PUREVOIP's verification practices include confirming a carrier customer's reported status in the FCC's Form 499 Filer database of registered carriers, and the Commission's Robocall Mitigation Database. PUREVOIP also conducts, as applicable, credit checks and checks references with a prospective customer's other carrier-suppliers.

As of January 2024, PUREVOIP only provides services to new customers that are incorporated in the United States and complete its Robocall Mitigation form. PUREVOIP cross-checks new customers' IPs against PUREVOIP's Media IP-block list. When PUREVOIP onboards new customers, PUREVOIP's fraud team also checks all new account traffic profiles for the first 24 hours by checking ANIs against databases such as YouMail and other proprietary and/or commercially available sources.

II. PUREVOIP's Acceptable Use Policy

As part of its customer-onboarding process, all of PUREVOIP's customers contractually agree to various terms and conditions, including a commitment to comply with PUREVOIP's Acceptable Use Policy (AUP). Among other things, this AUP prohibits:

- Using the Services to engage in any activities that are illegal, abusive, false, fraudulent, deceptive or misleading, or any activity that exploits, harms, or threatens to harm children.
- Using PUREVOIP's Services in any way that fails to conform to any applicable industry guidelines and standards, including, without limitation, the CTIA Messaging Principles and Best Practices, Short Code Registry Best Practices, and Short Code Monitoring Handbook.

- Creating a false identity, forged email address or header, phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call, including failing to comply with the Truth in Caller ID Act.

PUREVOIP's contracts with its customers stipulate that PUREVOIP is authorized to suspend and/or terminate all Services in the event of an AUP violation.

III. Telephone Number Authorization and STIR-SHAKEN Capabilities

PUREVOIP has fully implemented the STIR/SHAKEN authentication framework across its entire network. PUREVOIP's network accepts and accurately transmits all STIR/SHAKEN-related data it receives in the call path, consistent with 47 C.F.R. § 64.6302. As noted above, PUREVOIP provides its intermediate voice services solely to other registered domestic originating and intermediate voice service providers. As such, PUREVOIP is not the originating provider capable of authenticating the calling party's relationship with the caller ID ascribed to a given call, or to the called party.

IV. Proactive Network Monitoring

PUREVOIP has various monitoring and reporting systems in place to analyze traffic on its network for potentially suspicious traffic patterns that are likely to be associated with illegal robocalls or other potentially unlawful usage. For example, PUREVOIP's monitoring systems assess and, as applicable, flag or automatically block, traffic based on various criteria, including:

- (a) matching NPA-NXXs of the calling and called parties' telephone numbers;
- (b) calls with a caller ID of a telephone number associated with a wireless carrier from a customer understood not to carry wireless-originated traffic;
- (c) blocking calls for which the caller ID is not a valid, in-service ANI in the LERG;
- (d) blocking calls purporting to be from a telephone number on Somos' DNO list;
- (e) blocking calls from any Media IP address associated with a known or reported illegal robocalling entity, including Media IP addresses sourced from PUREVOIP's affiliate's proprietary, FraudCentral robocall-mitigation suite of tools; see <https://fraudcentral.io>; which leverages far more robust, sweeping and effective mitigation than traditional ANI-based tools have offered to date; and

PUREVOIP also declines to carry calls in real time via third-party mitigation tools and services provided via its underlying switch provider. PUREVOIP has a fraud department that operates around the clock and that monitors YouMail statistics and blocks the Media IPs of known bad actors to prevent such traffic from entering PUREVOIP's network, regardless of the carrier or phone number that the call(s) comes from.

PUREVOIP actively monitors and enforces these and other proprietary practices and policies designed to mitigate the misuse of its network. PUREVOIP requires its carrier customers to investigate and as applicable suspend or terminate their subject downstream customer promptly, and advise PUREVOIP of the actions taken to mitigate the issues raised in the traceback, and to remove similar types of traffic from PUREVOIP's network. If PUREVOIP receives a second traceback within 60 days of the first traceback regarding the same customer and campaign type, the customer is terminated immediately.

If PUREVOIP receives a general traceback related to a foreign customer, they are terminated immediately. If PUREVOIP receives notice from the Industry Traceback Group that its customer did not complete their traceback request, they are also suspended or terminated. If PUREVOIP receives knowledge, other than through a traceback, that a customer has allowed illegal traffic onto PUREVOIP's network, PUREVOIP warns its customer that they must immediately remove their underlying customer that generated the traffic.

If PUREVOIP detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, PUREVOIP takes prompt action to identify the party that is using its network to carry these calls and take appropriate action.

V. Commitment to Timely Traceback Responses and Cooperation

PUREVOIP commits to respond fully and in a timely manner, within 24 hours, to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate, carry, or process illegal robocalls. PUREVOIP will dedicate sufficient resources to provide timely and complete responses to such requests, and will investigate suspicious activity found by its monitoring systems or reported to it by appropriate parties and take appropriate action.