

ROBOCALL MITIGATION PLAN

Business Information

Plura Connect LLC
177 Cassia Way
Suite B112
Henderson, NV 89014

Contact Information

Daniel McKeehan
Chief Technology Officer
702-291-8243
dan@pluraconnect.ai

1. Overview

In the Commission's recent release, In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17-97 (rel. March 17, 2023) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that a RMP include:

- "know your customer" procedures;
- "know your upstream provider";
- ownership information;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that an RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

2. Introduction

Plura Connect LLC ("Plura Connect," "Plura") provides services to Plura AI LLC, an Internet SaaS telecommunications platform that facilitates the connection, transmission, and management of telecommunications services. As such, Plura is dedicated to combating illegal robocalls and fraudulent traffic, and has taken affirmative, effective measures to avoid originating, carrying, and processing illegal robocall traffic, as detailed herein.

Plura Connect is dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network. Plura Connect is currently in the process of implementing STIR/SHAKEN and is filing this robocall mitigation plan now because Robocall Mitigation Database registration is a prerequisite to obtaining an SPC Token required for STIR/SHAKEN implementation under the STI-PA policy. In compliance with the R&O, Plura Connect submits this RMP and certification.

3. Caller ID/Number Verification Controls

Using numbers not assigned to the caller (caller ID spoofing) is one of the primary mechanisms for illegal robocalls. To prevent this, Plura Connect independently verifies that any existing numbers to be used by customers are actually assigned to them prior to account approval and only allows customers to acquire new numbers directly from the Company.

4. Know Your Customer ("KYC")

(a) **Prospective Customer Review and Assessment:** Before a customer account can be approved for service, the business entity must be verified, along with the identities of the individual applying for the account and all users. The Company utilizes a third-party KYC verification service for this purpose, which also confirms the veracity of identity verification documents. A business entity must have an Employer Identification Number (EIN) or equivalent tax ID (e.g., social security) and provide a verifiable physical location for its place of business.

Individuals and business entities associated with an account may be further investigated by the Company's in-house legal department, which utilizes investigatory resources including WestLaw and LexisNexis to access official public records, business and fictitious name filings, domain registrations, and other records, to search for data that contradict the information provided by the prospective customer, or that might otherwise serve as a red flag.

Prospective customers must also provide a detailed description of how they intend to use the Company's services, anticipated monthly volume for each enabled service, and a detailed description of consumer contact data collection practices, including consent collection methodologies. All information submitted in connection with the intended use case is viewed with an eye towards ensuring that the prospective customer will utilize Company services solely as an end-user in full compliance with applicable statutes, rules, and regulations.

(b) **Certifications:** Each prospective Plura customer is required to certify:

- (i) Whether the business entity or any of its owners or users have been subject to any prior enforcements or judgments for alleged illegal activity.
 - (ii) That it has adopted internal compliance practices and procedures to ensure compliance with the Telephone Consumer Protection Act (TCPA), and any other applicable statute, rule, and regulation that applies to outbound calling and/or texting.
 - (iii) That it will fully cooperate with the Company in connection with any traceback requests or internal investigations of suspicious activity.
- (c) **Account Monitoring:** All approved and activated customer accounts are monitored on a regular ongoing basis for potentially unusual or suspicious usage, which may include:
- (i) ITG Traceback requests.
 - (ii) Reports of alleged improper communications as flagged by YouMail, or reported by downstream service providers, the general public, or others.
 - (iii) FCC and FTC consumer complaint data.
 - (iv) Flagged numbers that customers are unwilling or unable to remediate.
 - (v) Call traffic statistics, including short call duration percentage, average call duration, answer seizure ratio, etc. and
 - (vi) Requests for high capacity (calls per second or concurrent calls), particularly if disproportionate to the size of the account.
- (d) **Contractual Protections.** Among other restrictions, Plura customers are required to adhere to the terms of its Acceptable Use Policy (AUP) which outlines an extensive but non-exhaustive list of prohibited conduct. The Company's customer agreements grant it the right to suspend or terminate service for any customer suspected of violating the AUP or otherwise using the Company's services in a suspicious manner, as determined by the Company in its sole discretion. When suspected violations of the AUP or other contractual provisions occur, the Company's legal department evaluates the violation and takes appropriate enforcement action.

5. **Know Your Upstream Providers**

In accordance with 47 C.F.R § 64.6305(g)(1), Plura Connect only accepts calls directly from upstream providers that have filed a Robocall Mitigation Plan in the RMD, and that filing has not been de-listed pursuant to an enforcement action. To further minimize the likelihood of receiving illegal robocall traffic from an upstream provider, the Company:

- Only routes traffic using Tier 1 providers.
- Maintains a vetted list of approved upstream providers.
- Regularly monitors traffic patterns from each upstream provider.
- Implements traceback procedures to identify the source of suspicious traffic.

In addition to the operational measures described above, Plura Connect conditions its relationships with upstream providers on written agreements that require such providers to: (i) maintain a current, accurate, and non-delisted Robocall Mitigation Database filing with the FCC; (ii) implement and enforce their own robocall mitigation and STIR/SHAKEN authentication programs consistent with applicable FCC rules; (iii) fully cooperate with the Company, the ITG, the FCC, and law enforcement in connection with traceback and related investigations, including timely provision of call records and other relevant information; and (iv) refrain from originating, carrying, or processing illegal robocalls or unlawfully spoofed traffic. These agreements expressly authorize the Company to immediately suspend or terminate the routing of traffic from any upstream provider that fails to meet these obligations or that is reasonably suspected of transmitting illegal or noncompliant traffic.

6. Call Analytics and Blocking

All calls originating from the Company's network are analyzed internally and through third-party analytics vendors to identify and prevent illegal robocall traffic.

(a) **Internal Analytics Methodologies:** Plura's internal analysis methodologies includes monitoring real time call traffic patterns on its network to detect patterns indicative of potential illegal call traffic, such as high call volumes from a single source. Calls that exceed thresholds are flagged or blocked dynamically. The Company also utilizes AI-powered systems to analyze large datasets to detect patterns associated with robocalls, such as repetitive call attempts or known scam tactics. These automated detection methods are supplemented by intensive manual reviews of customer accounts that have been flagged as suspicious.

(b) **Third Party Analytics Providers:**

- (i) **YouMail:** YouMail is known within the telecommunications industry for its analytics offerings and partners closely with the Industry Traceback Group (ITG), the FCC, and other law enforcement authorities. The Company utilizes YouMail's Watch service, a robust solution designed to detect and mitigate illegal robocall traffic and other harmful activities on carrier networks that leverages YouMail's extensive sensor network, including over 10 million active users and millions of "honeypot" numbers, to identify problematic call traffic.
- (ii) **SOMOS:** Somos offers a range of services to voice service providers aimed at ensuring trust, transparency, and security in telecommunications. The Company utilizes the Somos RealNumber Do Not Originate (DNO) database to identify phone numbers marked as DNO, and blocks all numbers listed on this database, which include those reported as inbound only by providers, numbers unused by customers as reported by providers, and numbers designated as inbound only by

customers. The Company also accesses real-time updates to the SOMOS DNO database to ensure call screening accuracy.

7. Blocking

Plura Connect will promptly respond to Do Not Originate requests it receives from ITG. Plura Connect has mechanisms to automatically block suspicious calls using internal analytics. If Plura Connect's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Plura Connect will take appropriate action which may include suspending or terminating the subscriber's use of Plura Connect's network. Plura Connect will cooperate with investigative bodies (provide a single point of contact to address traceback requests from law enforcement including state attorneys general offices), to the FCC, and/or ITG; as well as documenting requests and actions taken in response thereto. Plura Connect will respond to traceback requests within 24 hours.

Pursuant to 47 CFR § 64.1200(p), the Company utilizes the Somos RealNumber Do Not Originate (DNO) database to identify phone numbers marked as DNO, and blocks all numbers identified by Somos as invalid, unallocated, unused, or inbound-only government or private numbers. The Company also accesses real-time updates to the SOMOS DNO database to ensure call screening accuracy.

Publicly Available Error Reporting Mechanism: The Company has established a dedicated email address (blocking@verificationtechnologies.ai) to receive reports of erroneous blocking from customers and other voice service providers. This information is published on the Company's public-facing website, <https://www.verificationtechnologies.ai>.

8. Plan Updates

This plan, along with industry best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. Plura Connect will monitor industry best practices and continuously improve our internal processes to ensure this plan, and our system adapts to this ever-changing issue.

In the event of any material change to this plan, Plura Connect will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of Matthew Beucler

I, Matthew Beucler, Chief Operating Officer of Plura Connect LLC ("Plura Connect"), do hereby certify, under penalty of perjury, the following:

- (1) Plura Connect is currently in the process of implementing STIR/SHAKEN and is filing this robocall mitigation plan now because Robocall Mitigation Database registration is a prerequisite to obtaining an SPC Token required for STIR/SHAKEN implementation under the STI-PA policy.
- (2) Plura Connect's Business name and primary address are as follows:

Plura Connect LLC
177 Cassia Way
Suite B112
Carlsbad, CA 92011
- (3) Plura Connect does not use any other business names
- (4) Plura Connect has not previously used any other business name.
- (5) The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- (6) Plura Connect has the following parent company: Plura Holdings, LLC.
- (7) The following persons exercise management and control over Plura Connect: Matthew Beucler, Seth Heyman, Daniel McKeehan.
- (8) Plura Connect has the following affiliates: Plura AI LLC.
- (9) None of the persons/entities in items 5 – 7 above have had any licenses denied or revoked by the FCC or been subject to an FCC enforcement proceeding.
- (10) Plura Connect's role in the call chain is that of (a) a Voice Service Provider with a STIR/SHAKEN implementation obligation serving end-users and (b) a Non-Gateway Intermediate Provider with a STIR/SHAKEN obligation.
- (11) Plura Connect has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.

- (12) Plura Connect is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

A handwritten signature in black ink, appearing to read "Matthew Beucler", written over a horizontal line.

Matthew Beucler