

ROBOCALL MITIGATION PLAN

IDENTIFICATION AND CONTACT INFORMATION:

Business Name: Reynwood Communications of NY/NJ, LLC
Address: 409 South Street, Unit 1128
Eatontown, NJ 07724

ROBOCALL MITIGATION CONTACT:

Name: Patricia Diggins, CFO
Email: patty@reynwood.com
Phone: 732.924.4085

Principals: Richard Kelly, Patricia Diggins
RCL has no parent company, affiliates, or subsidiaries.

I. OVERVIEW

Reynwood Communications of NY/NJ, LLC (RCL) is committed to complying with the requirements outlined in the Commission's robocall rules and orders. This robocall mitigation plan ("plan") details RCL's steps to prevent the origination of illegal robocalls, ensure timely traceback responses, and meet all filing obligations in the Robocall Mitigation Database (RMD).

RCL is a competitive local exchange carrier and Hosted VoIP Provider for commercial clients nationwide. This plan applies to all calls originating on and traversing RCL's network.

II. GENERAL PROHIBITION AGAINST ILLEGAL ROBOCALLING

RCL end-user services are subject to restrictions contained in its published legal notices and all executed service orders include the requirement that service is provided according to its terms of service ("TOS") requirements. Its existing TOS prohibits activities usually associated with Robocalling, including, but not limited to:

- Providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call; and
- violating any applicable local, state, or federal law; using the RCL service to engage in or in connection with fraudulent activities.

In addition, the company has updated its TOS to expressly reference the prohibition on robocalling, and all current subscribers have received notice of the publication of its updated TOS. RCL's end users are notified that RCL may take action up to suspension or termination of service for violation of the TOS.

III. COMPLIANCE WITH SIXTH CALLER ID AUTHENTICATION ORDER

The **Sixth Caller ID Authentication Order**, *Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, 38 FCC Rcd 2573 (2023), introduced enhanced

information requirements for RMD certifications. RCL ensures compliance by implementing the following:

ROBOCALL MITIGATION CERTIFICATION:

- RCL certifies that all calls originating on its network are subject to a comprehensive robocall mitigation program.
- Certification filed in the FCC's RMD includes:
 - Declaration of robocall status.
 - Confirmation that prior certifications have not been removed by Commission action.

DETAILED ROBOCALL MITIGATION PLAN:

PREVENTATIVE MEASURES:

- **Know Your Customer (KYC):** RCL is a small, long-established provider with close relationships with its subscribers. Its clients are generally small- to medium-sized businesses and governmental agencies, and few of its clients have enough call paths to generate the high volume of traffic associated with robocalling, allowing us to use targeted in-house analytics to monitor, alert, and apprehend suspected robocalling activities. To strengthen its mitigation efforts, RCL verifies each client's **address and contact information** and conducts a **site visit** before enabling outbound calling.
- **Network Monitoring:** RCL employs real-time monitoring to detect suspicious call patterns.
- **Call Path Limits:** Large volume calling capabilities are NEVER provisioned on our network.
- **Telephone Number Authorization:** A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify the caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by RCL and/or obtained by RCL from one of RCL's underlying carriers for use by the subscriber. In most cases, RCL directly manages the TNs used by its subscribers. RCL tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of RCL's assignment of the TN to its subscriber. If a subscriber wishes to use a TN as a caller identity and that TN is not directly managed by RCL, then TN validation is necessary. If a subscriber's end-user can provide a valid letter of authorization that they are the authorized user of such TNs, RCL will attest calls originated with these TNs. When originating a call, RCL checks the calling party number against RCL's inventory and will not attest the call unless the calling party number is a TN that has been properly validated

CALL ANALYTICS SYSTEMS:

RCL employs in-house analytics and third-party systems to:

- Identify and flag potential robocall traffic.
- Automatically disable accounts associated with suspicious activity.

THIRD-PARTY VENDORS THAT ASSIST IN DEPLOYING CALL ANALYTICS:

- Oracle Communications

- TransNexus
- Cisco Broadworks
- Averistar

TRACEBACK COMMITMENT:

RCL commits to responding to traceback requests within **24 hours**.

DISCLOSURE OF PRIOR ACTIONS:

RCL certifies that it has not been the subject of FCC or law enforcement actions due to robocall legal or administrative rule violations.

RCL further certifies that it has not been prohibited from filing in the Robocall Mitigation Database for any reason.

IV. COMPLIANCE WITH THE SEVENTH CALL BLOCKING ORDER

The **Seventh Call Blocking Order**, *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, Seventh Report and Order*, FCC 23-37 (2023) expanded obligations to include stricter robocall mitigation and blocking requirements. RCL ensures compliance with the following measures:

COMMITMENT TO FULL TRACEBACK COOPERATION:

- RCL responds to traceback requests from the **FCC, Industry Traceback Group (ITG)**, or law enforcement agencies within **24 hours**.
- Dedicated staff and resources ensure prompt, accurate responses.

BLOCKING OF SUSPICIOUS TRAFFIC:

- RCL's systems are configured to automatically:
 - Identify and block calls with patterns indicative of illegal robocalling.
 - Manually review call details records of suspected robocalling activities.
 - Suspend services of customers engaged in robocalling activities.

PREVENTION OF NEW AND RENEWING CUSTOMERS FROM ORIGINATING ILLEGAL ROBOCALLS:

- All new customers undergo rigorous KYC verification, including:
 - **Tax ID validation.**
 - **Business type verification.**
 - **Address validation** to prevent deployment of large-volume capabilities to residential addresses.
- Existing customers with higher-volume capabilities are subject to periodic compliance reviews.

CALL ANALYTICS AND MONITORING:

- **In-House Analytics System:**
 - Monitors traffic in real-time.
 - Flags high-volume call patterns resembling robocall campaigns.

- Automatically disables flagged accounts pending review.
- **Third-Party Call Analytics:**
 - Additional layer of fraud detection and blocking.

V. DETAILED ROBOCALL MITIGATION STEPS

END-USER COMPLIANCE

- Terms of Service (TOS) explicitly prohibit:
 - Deceptive caller ID practices.
 - Illegal robocalling and spoofing activities.
 - Violations result in immediate suspension or termination of service.

NETWORK TRAFFIC MONITORING

- Continuous real-time monitoring of call traffic.
- Flagging and blocking of suspicious call patterns.
- Logging of all blocked calls for audit and review purposes.

TRACEBACK PROCEDURES

- Dedicated team ensures full cooperation with traceback requests within 24 hours.
- Immediate investigation and remediation of any flagged traffic.

UPSTREAM PROVIDER VERIFICATION

- RCL's upstream carriers are:
 - Verizon
5055 North Point Pkwy, NP2NE Network Eng
Alpharetta GA 30022
Phillip Lin
(800) 229-7427
caryrobomanagement@verizon.com
 - Lumen Technologies, Inc.
100 CenturyLink Dr.
Mailstop: 3TCW88.2
Monroe LA 71203
Philip Linse
(303)707-3844
philip.linse@lumen.com
- RCL verifies upstream providers to ensure they have:
 - Valid RMD certifications.
 - Effective robocall mitigation policies.

VI. COMPLIANCE DECLARATION

RCL certifies the following:

- **All calls** originating on our network are subject to our robocall mitigation program.
- RCL's role in that of a voice service provider that does not have a STIR/SHAKEN obligation.
- RCL complies with the **Sixth Caller ID Authentication Order** and **Seventh Call Blocking Order requirements, as well as all other Commission rules and orders concerning robocall mitigation.**
- RCL has **not** been subject to enforcement action related to robocalls in the past two years.

This plan will be updated within 10 days of any change in the items listed herein, to ensure ongoing compliance.