

v9 Communications Corporation (V9) is a small Voice Over Internet Provider that is dedicated to stopping illegal calls from originating in our network.

V9 has taken the specific reasonable steps set forth in this document to avoid originating illegal robocall traffic as part of its RMP. V9 is continuously analyzing the effectiveness of this plan and reviewing best practices. V9 reserves the right to modify and/or supplement the robocall mitigation measures included here to adapt to risks from bad actors and to improve the overall effectiveness of its program for the benefit of its customers.

Any voice traffic that originates on our network is subject to the RMP as described below.

Know Your Customer

V9 employs a variety of “know-your-customer” initiatives to help mitigate the risk that its customers would attempt to use V9’s network to initiate illegal robocalling campaigns. V9 makes reasonable, good faith efforts to validate the identity of its customers. These measures include, but are not limited to, collecting information such as physical business location, contact person(s), and the nature of the customer’s business. V9 does not automate (self-service) any portion of the establishment, sale, provisioning, and authorization of service procured on our network. These measures help prevent bad actors from becoming V9 customers and reduce the likelihood that V9 will inadvertently carry illegal robocall traffic.

Acceptable Use Policy

V9’s service agreements contain acceptable use terms (AUP) that prohibit using V9’s services for illegal purposes.

Traceback Requests

V9 commits to respond fully and in a timely manner 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 may use its service to originate calls.

Telephone Number Validation

If a subscriber wishes to use a telephone number (TN) as a caller identity and that TN is not directly managed by V9, then TN validation is necessary by requiring the subscriber to provide a valid letter of authorization that they are an authorized user of such TN.

Network Monitoring Practices

Our origination voice traffic is monitored in real time to prevent the origination of illegal robocalls and fraud.

Examples of calling patterns monitored:

- Higher than expected cost generated by calls from a subscriber
- Targeted pumping of repeated calls to a specific called number.
- Fast traffic pumping of repeated calls to a specific called geographic location.
- Slow traffic pumping of repeated calls to a specific called geographic location.
- Theft of service traffic pumping of repeated calls to high-cost geographic location.
- Recent call volumes vs. weekly trends
- Number of unique destination numbers in a time frame.
- Irregularities in Short Call Duration and Average Call Duration distribution.
- Anomalies in Answer-Seizure Ratio.

- Analysis of recent and past Call Detail Records to benchmark against expected trends.

The solution provides detailed reporting identifying suspected illegal robocalls and alerts Provider if we originate any calls where the calling number is invalid, unallocated, or on a Do Not Originate list. V9 will investigate any identified calls to determine if the caller was attempting to originate unlawful robocalls. If V9 determines that the caller was attempting to originate unlawful robocalls, then we either warn them to stop or terminate their service as based on our AUP.