

Robocall Mitigation Plan

Business Information

Login, LLC
1855 N. 6th Avenue
Tucson, AZ 85705

Contact Information

Scott Harvanek
Vice President Operations
520-618-3000
traceback@loginbusiness.com

Overview

The FCC requires that all voice service providers (“VSPs”) certify in the Robocall Mitigation Database that they have implemented a Robocall Mitigation Plan (“RMP”) to ensure that they are not originating illegal robocalls. The FCC requires that VSPs develop a RMP that:

- details the reasonable steps taken to avoid originating illegal robocalls;
- demonstrates a commitment to respond to traceback requests to cooperate with investigators and stopping illegal robocalls; and
- is filed in the Robocall Mitigation Database.

The FCC states that a 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.

Purpose

Login, LLC (“Login”) is a small VSP that is dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. This document delineates Login’s RMP.

Know Your Customer

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with Login in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

New Subscribers

All new subscribers go through identity verification protocols. A risk score is developed to ensure the authenticity of a new subscriber. This score checks the identity marker collected during an account registration process. These include but are not limited to: name, email address, credit card information and contact phone number. These identity markers are validated for accuracy against public and paid tools. All new subscriber activity is monitored as further explained below.

Existing Subscribers

Login requires updates of subscribers' information on all their orders. Each order's identity markers are verified again to ensure the account is not compromised and is being used for its intended purpose.

Acceptable Use Policy

Login maintains an Acceptable Use Policy ("AUP") that subscribers must sign before being permitted to use Login's network. Among other things, this AUP prohibits falsifying header information or user identification information, which Login interprets to include caller identification data. It also forbids violating any applicable law, regulation, treaty, or tariff, as well as violating the acceptable use policies of any networks, machines, or services accessed through Login's network. Finally, the policy strictly restricts users from transmitting, distributing, or storing information or material that is fraudulent or contains false, deceptive, or misleading statements.

Telephone Number Authorization & STIR/SHAKEN Attestation

A telephone number-based caller identity is the originating phone number included in call signaling, which uniquely identifies the caller for network screening purposes. A subscriber is permitted to use a specific telephone number as their caller identity only if the number is directly managed by Login or explicitly obtained by our team from an underlying carrier on the subscriber's behalf.

To ensure full accountability for our numbering resources and to actively prevent attestation laundering, Login maintains its own Service Provider Code token and operates a proprietary STIR/SHAKEN certificate. We do not rely on third-party upstream providers to sign our calls. Instead, we directly sign and vouch for the legitimacy of traffic originating from our network, applying an A-Level attestation or another appropriate level based on our strict Know Your Customer protocols.

In most instances, Login directly manages the telephone numbers used by our subscribers. Our compliance engine tracks these numbers within our inventory system and monitors their assignment, making validation an inherent result of the provisioning process. However, if a subscriber wishes to use a caller identity that is not directly managed by our network, explicit validation is required. The subscriber must provide a valid letter of authorization proving they have the legal right to use that specific number. When originating any call, our system automatically checks the calling party number against our active inventory. Login will strictly withhold A-Level attestation, or block the call entirely, unless the caller identity has been thoroughly validated by our team.

Mitigation Through Contracts

Login contractually enforces our robocall mitigation efforts by requiring all subscribers to actively participate in traceback requests. This mandatory cooperation is an explicit provision within our continuously binding Terms of Use. A customer's continued use of our network constitutes their ongoing agreement to these terms, our acceptable use policies, and any subsequent updates.

Quantitative Monitoring Architecture

Login employs a dedicated, automated compliance engine that analyzes 100% of outbound traffic. Our compliance engine serves as the active operational system enforcing Login's Robocall Mitigation Plan. To ensure continuous, automated surveillance of network traffic, the software extracts and normalizes raw billing data from our underlying carriers into a single analysis stream. This data then flows directly into a metric calculation engine, which applies industry-standard formulas to derive critical quality indicators. Specifically, it calculates the Answer Seizure Ratio (ASR), the Average Call Duration (ACD), and the percentage of Short Duration Calls (SDC) lasting under 15 seconds, which often indicate spam or neighbor spoofing activity.

The final component of the compliance engine acts as the operational decision-maker by comparing these metrics against hard-coded thresholds. On a global network level, the system triggers warnings if the overall ASR drops below 40.0%, the ACD falls under 15.0 seconds, or the SDC ratio exceeds 20.0%. Furthermore, it enforces "Know Your Traffic" (KYT) rules on a per-number basis for any originating number exceeding 50 calls in a 24-hour period. Specific triggers include an ASR under 20.0% (indicating potential Spam or Wangiri Fraud), an SDC ratio over 50.0% (suggesting Neighbor Spoofing), or an ACD under 6.0 seconds (pointing to

Autodialer or Robocall Blast activity). When a violation occurs, the system immediately generates an actionable alert for network operations to begin the investigation protocol.

Automated Alerting & Remediation Protocol

When the compliance engine detects a violation of the defined thresholds, it automatically generates an internal suspicious actor event. Upon this alert generation, Login initiates a mandatory 24-hour investigation cycle. During the first four hours of this cycle, our compliance staff verifies the call detail record data against the specific thresholds, such as confirming if the short duration call ratio exceeds 50 percent. Over the subsequent 20 hours, our team contacts the subscriber, who must then provide a verified explanation for the traffic patterns, such as school closures or appointment reminders, or supply valid consent documentation. Accounts found with a short duration call ratio exceeding 80 percent or those engaged in blatant impersonation face immediate suspension without notice. Finally, if a subscriber fails to provide a satisfactory response or cure the violation within the 24-hour period, their service is terminated.

Blocking

Login will implement Do Not Originate (DNO) requests it receives from the Industry Traceback Group (ITG). If our compliance engine identifies suspected robocalling patterns that are confirmed through further investigation, Login will take immediate action, which may include suspending or terminating the subscriber's access to our network. Login actively cooperates with all investigative bodies and maintains a designated single point of contact to promptly address traceback requests from law enforcement, state attorneys general, the FCC, and the ITG. Furthermore, we comprehensively document all traceback requests and the subsequent actions taken in response.

Plan Updates & Annual Recertification

This mitigation plan and our internal strategies must continuously evolve to address the dynamic nature of illegal robocalling. Login actively monitors emerging threats and industry standards to ensure our compliance engine and operational protocols adapt to this ever-changing landscape. In the event of any material change to this plan or our corporate business information, Login will republish the updated policies to all relevant employees, consultants, and contractors, and we will file the necessary updates to the FCC Robocall Mitigation Database and the CORES system within ten business days. Furthermore, in strict adherence to FCC regulations, Login commits to recertifying the accuracy of our comprehensive Robocall Mitigation Database submission annually by the March 1 deadline.