

Robocall Mitigation Plan

Business Information

Popcorn Labs, Inc.
110 E 25th Street
New York, NY 10010

Contact Information

Neel Popat, CEO
110 East 25th Street,
New York, NY 10010
Phone: 213-932-9978
Email: Neel@popcorn.space

Overview

In the Commission's release, *Call Authentication Trust Anchor*, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd. 2573 (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 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

Popcorn Labs, Inc. ("Popcorn Labs") is a small VSP dedicated to stopping illegal calls from traversing our network and monitoring the calls coming into our network. Popcorn Labs is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, Popcorn Labs was previously exempt from the FCC's STIR/SHAKEN rules. The R&O requires that pure resellers such as Popcorn Labs now file RMPs. This document delineates Popcorn Labs's RMP. Because Popcorn Labs does not have access to the necessary infrastructure, it relies on its upstream carrier to assist in robocall mitigation. As delineated herein, Popcorn Labs works closely with its upstream provider to carry out the required mitigation functions.

Know Your Customer ("KYC")

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 Popcorn Labs in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

Popcorn Labs's KYC program involves obtaining specific subscriber information when payment is made for services. This process includes collecting such information such as:

- email address;
- home location (for residential customers);
- corporate location (for business customers);
- contact person(s)' first and last name(s);
- payment details (via Stripe);
- nature of the customer's business (for business customers).

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls, and Call Authentication Trust Anchor*, Seventh Report and Order in CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59, 38 FCC Rcd 5404 (2023), Popcorn Labs provides the following information concerning its upstream voice service carrier.

Popcorn Labs has one upstream provider from which it receives voice traffic:

T-Mobile USA, Inc.
12920 SE 38th Street
Bellevue WA 98006
Shilpa Bhanot
214-305-7095
RobocallMitigationSupport@T-Mobile.com¹

Popcorn Labs has received assurances from its upstream carrier that it has, and will continue to, sign calls transmitted to Popcorn Labs and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Popcorn Labs. Popcorn Labs and its upstream provider have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

Popcorn Labs maintains an AUP that subscribers must sign before being permitted to use Popcorn Labs's network. Among other things, the AUP prohibits:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- violating any applicable local, state, or federal law;
- violating applicable industry accepted guidelines; and
- using Popcorn Labs's service to engage in or in connection with fraudulent activities.

¹ Popcorn Labs has a master service agreement with MVNO Connect, LLC ("MVNO"). As stated in that master service agreement, MVNO uses the infrastructure of T-Mobile USA, Inc.'s ("T-Mobile") for call routing and attestation. T-Mobile is STIR/SHAKEN compliant, and signs all of Popcorn's calls vis-a-vis MVNO's use of T-Mobile's infrastructure. T-Mobile's robocall mitigation plan, attached to its filing RMD0004209, elaborates on this scenario in the plan's section on T-Mobile's agreements with virtual mobile service operator partners. Accordingly, for the purposes of this RMP, T-Mobile is Popcorn Labs's upstream carrier.

Popcorn Labs's contractual terms with subscribers specify that Popcorn Labs may take action up to suspension or termination of service for violation of the AUP.

Mitigation During Service

Popcorn Labs works with its upstream provider to ensure that all subscribers can report any suspicious call connected through their account and measures are set to prevent future calls from/to that individual numbers for all subscribers (none routed by the platform from that moment on - blacklisting). These features are:

- VoIP-originated calls are signed with subscriber caller ID only after number validation; and
- requiring authentication to initiate any call, or a whitelist of originating numbers that is under customer's control.

Analytics for Monitoring Traffic

Popcorn Labs works with its upstream provider to identify behaviors which indicate illegal call activity. Examples of calling patterns monitored:

- anomalies in cost generated by calls from a single customer;
- multiple overlapping calls on the same account is a risk of not having a single subscriber using the service;
- velocity on initiate calls (synchron intervals, quick dialing back-to-back calls);
- recent volumes (last 60 min) vs weekly trends;
- number of unique destination numbers in a time frame (total account level);
- number of unique source numbers in a time frame (total and account level); and
- anomalies in call duration distribution (most calls having similar duration is not representative for residential service usage).

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Popcorn Labs works with its upstream provider to follow defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his particular use case and validate that the activity belongs to that subscriber.

Because Popcorn Labs does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in Popcorn Labs's analytics.

Popcorn Labs follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Popcorn Labs will devote sufficient resources to provide prompt and complete resources to traceback requests. Popcorn Labs commits to responding to traceback requests fully within 24 hours.

Popcorn Labs works with its upstream provider to investigate suspicious activity found by the carrier's monitoring systems or reported to Popcorn Labs by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Popcorn Labs contacting a subscriber to correct improper use of the applicable platform, or, if the subscriber does not respond or comply, to notify its upstream provider to block their use of the platform.

For all new and renegotiated Popcorn Labs contracts governing the transport of voice calls, Popcorn Labs will endeavor to contractually require Popcorn Labs's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Popcorn Labs will implement Do Not Originate requests it receives from ITG. Popcorn Labs's upstream provider has mechanisms to automatically block suspicious calls using internal analytics. If Popcorn Labs and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, Popcorn Labs will take appropriate action which may include suspending or terminating the subscriber's use of Popcorn Labs Popcorn Labs's service. Popcorn Labs will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including the state attorney general's office), as well as the FCC, and/or ITG; as well as documenting requests & actions taken in response thereto.

Plan Updates

This plan, along with industry best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. Popcorn Labs 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, Popcorn Labs 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. **Popcorn Labs recertifies that it has reviewed the contents of this plan and its current filing RMD filing and confirms that all the information therein is current and complete as of March 1, 2026 and the date of this filing.**

Certification of Neel Popat

I, Neel Popat, CEO of Popcorn Labs, do hereby certify, under penalty of perjury, the following:

- Popcorn Labs, Inc. ("Popcorn Labs"), by virtue of its status as a "pure reseller" does not have access to the necessary infrastructure to implement STIR/SHAKEN, and therefore has not implemented STIR/SHAKEN in the IP portions of its network.
- Popcorn Labs 's Business name and primary address are as follows:

Popcorn Labs, Inc.
110 E 25th Street
New York, NY 10010
- Popcorn Labs has no other business names in use.
- Popcorn Labs has not previously used any other business name.
- The following persons/entities own more than 10% of Popcorn Labs each: Neel Popat, Lukas Kairys.
- The following persons are principals of Popcorn Labs: Neel Popat, Lukas Kairys.
- Popcorn Labs has no subsidiaries or affiliates.
- None of the persons/entities listed above have had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- 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.
- Popcorn Labs's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- Popcorn Labs has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- Popcorn Labs is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- Popcorn Labs is not required to have, and does not have, an operating company number.

Neel Popat

3/12/2026