

Robocall Mitigation Plan

Business Information

Callingly LLC
12621 N. Tatum Blvd., Suite 415
Phoenix, AZ 85032

Contact Information

Leon Klepfish
CEO
602-481-9661
leon@callingly.com

Overview

In the Commission's recent 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

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

Callingly is a speed-to-lead platform used by identified B2C sales teams to return calls to their own inbound leads; we do not sell bulk or cold dialing capacity. We take reasonable steps to mitigate illegal robocalls. For example, our platform restricts calls outside of allowed calling hours, with a contractual duty on the customer to observe that window in all cases. Besides, manual outbound dialing is disabled for the first 12 hours of a new account and blocked entirely on fraud-flagged

accounts; Caller IDs to leads are restricted to numbers we provision or to those the customer PIN-verifies; we have a per-customer Twilio subaccount isolation and hourly monitor caller-ID block-rate with automatic repointing.

Know Your Customer ("KYC")

Callingly requires each prospective customer to register using a business email address. Email addresses associated with free providers or disposable domains are screened through a third-party reputation service and rejected. During registration, Callingly records the user's IP address, country, and time zone, and the reputation service evaluates each signup for device- and identity-related fraud indicators. If the service does not return a "Real" verdict, the account is flagged and outbound calling is disabled until Callingly personnel complete a manual verification review. Before a customer may send messages or register a brand, Callingly collects and verifies the customer's legal business name, employer identification number (EIN), business type, registered address, website, industry, and the identity of an authorized representative. The business name, EIN, and address are validated through Twilio Trust Hub review and an independent review by Callingly staff. Caller ID numbers must either be provisioned by Callingly or verified through a PIN-based process. In addition, each account must be billed through Stripe to a payment card associated with a named cardholder; Callingly does not permit anonymous or prepaid account arrangements.

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), Callingly provides the following information concerning its upstream voice service carrier.

Callingly has two upstream providers from which it receives voice traffic:

- 1) Twilio, Inc.
101 Spear St., 1st Floor, San Francisco, CA 94105
Paul Kenefick
regulatory-north-america@twilio.com
- 2) Bandwidth, Inc.
900 Main Campus Dr., Raleigh, NC 27606
Stephen Thayer
voicsecurity@bandwidth.com

Callingly has master service agreements with its upstream providers and has received assurances in writing from their officials that they have and will continue to, sign calls transmitted to Callingly and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Callingly. Callingly and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

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

- Violating any applicable law or regulation, including the TCPA, the Truth in Caller ID Act, the Telemarketing Sales Rule, and state telemarketing and recording statutes.
- Originating illegal robocalls, or any call or message that is fraudulent, deceptive, or intended to mislead the recipient about who is calling or why.
- Conducting phishing, vishing, smishing, or any scheme to obtain credentials, financial details, one-time passcodes, or other sensitive information under false pretenses.
- Impersonating Callingly, a Callingly employee, a government agency, a financial institution, a carrier, or any other person or entity.
- Harassing, threatening, defaming, or abusing any person, or contacting a person after they have asked the caller to stop.
- Marketing unlawful goods or services, or running lead-generation for any of them. Exploiting or harming minors, or directing traffic to numbers the caller knows or should know belong to minors. Engaging in traffic pumping, access stimulation, or any scheme to generate artificial call volume for revenue.

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

Mitigation During Service

Callingly works with its upstream providers to ensure that all subscribers can report any suspicious call connected through their account.

Callingly receives complaints, carrier notifications, and traceback requests through abuse@callingly.com and triages each matter on the same business day. To support prompt investigation and attribution, Callingly retains detailed records for every call leg, including the call SID, originating caller ID, called number, date and time, originating customer account, and individual user. Each customer operates within a separate Twilio subaccount, enabling Callingly to associate a telephone number and timestamp with a specific, verified customer and to retrieve any available call recording and transcript. Callingly also incorporates automated risk indicators into its monitoring and escalation process. Caller ID health is reviewed hourly to identify numbers that terminating carriers may be blocking or rejecting, while signup fraud assessments and A2P registration reviews are routed to a monitored internal channel for evaluation. If Callingly determines that a customer has originated traffic in violation of its Terms of Service, Callingly promptly suspends the customer's outbound dialing privileges, revokes its caller IDs, and releases its telephone numbers. Callingly also cooperates fully with its upstream service providers and appropriate law enforcement authorities in connection with investigations and mitigation efforts.

Analytics for Monitoring Traffic

Callingly works with its upstream providers to identify behaviors which indicate illegal call activity. Because Callingly does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in Callingly's analytics.

Investigate Suspicious Activity

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

Callingly follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Callingly will devote sufficient resources to provide prompt and complete resources to traceback requests. Callingly commits to respond within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

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

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

Blocking

Callingly will implement Do Not Originate requests received from ITG, our upstream providers, or directly actioned by our compliance contact. Callingly's upstream providers have mechanisms to automatically block suspicious calls using internal analytics. If Callingly and/or its upstream carriers identify suspected robocalling patterns that are confirmed with further investigation, Callingly will take appropriate action which may include suspending or terminating the subscriber's use of Callingly's service. Callingly 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. Callingly 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, Callingly 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 Leon Klepfish

I, Leon Klepfish, CEO of Callingly LLC, do hereby certify, under penalty of perjury, the following:

- (1) Callingly LLC ("Callingly"), 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.
- (2) Callingly's Business name and primary address are as follows:

Callingly LLC
12621 N. Tatum Blvd., Suite 415, Phoenix, AZ 85032
- (3) Callingly has no other business names in use.
- (4) Callingly has not previously used any other business name.
- (5) Leon Klepfish is the sole person owning more than 10% of Callingly and exercising management and control over Callingly. He hasn't had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (6) Callingly has no subsidiaries or affiliates.
- (7) 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.
- (8) Callingly's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (9) Callingly has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (10) Callingly is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (11) Callingly is not required to have, and does not have an operating company number.

Leon Klepfish

Leon Klepfish

09/25/2026