

Robocall Mitigation Plan

Business Information

Telecom Evolutions, LLC
9221 Corbin Avenue Suite 155,
Northridge, CA 91324

Contact Information

James Murphy
Chief Executive Officer
818.264.4405
jim@broadvoice.com

Overview

In the Commission's release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 2023) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outlines "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

Telecom Evolutions, LLC ("TE") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. Because TE lacks control of the infrastructure necessary to implement STIR/SHAKEN, it is not required to be STIR/SHAKEN compliant. In compliance with the R&O, TE submits this RMP and certification.

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 TE 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 which are a mixture of algorithmic check and manual call back. 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

TE require 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

TE maintains an Acceptable Use Policy ("AUP") that subscribers must agree to before being permitted to use TE's network. Among other things, this 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 TE's service to engage in or in connection with fraudulent activities.

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

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 TE and/or obtained by TE from one of TE's underlying carriers for use by the subscriber. In most cases, TE directly manages the TNs used by its subscribers. TE tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of TE'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 TE, 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, TE will attest calls originated with these TNs.

When originating a call, TE checks the calling party number against TE's inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

Mitigation Through Contracts

All subscribers agree to participate in traceback requests (this is part of the Terms and Conditions which users must agree to when creating an account with us).

During Service

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 via SMS; and
- Requiring authentication to initiate any call, or a whitelist of originating numbers that is under customer's control.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls 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* (Rel. May 19, 2023) ¶¶ 49-51, TE provides the following information concerning its upstream voice service carrier.

TE's upstream provider is:

Syndeo LLC
9221 Corbin Ave.
Suite 260
Northridge, CA 91324
George Mitsopoulos
george@broadvoice.com

TE and its upstream provider has no contractual provisions regarding robocall mitigation. But TE and its upstream provider work together to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests. TE's upstream provider is listed as STIR/SHAKEN compliant in the Robocall Mitigation Database.

Monitor Traffic with Analytics

Dynamic Traffic Analysis identifies 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).

No third-party vendors are involved in deploying TE's analytics.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, our risk prevention team is alerted which follows the 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.

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

TE will investigate suspicious activity found by its monitoring systems or reported to TE by subscribers or third parties. The investigation could potentially result in opening a traceback request or with TE contacting a subscriber to correct improper use of the platform, or, if the subscriber does not respond or comply, to block their use of the platform.

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

Blocking

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

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. TE will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

In the event of any material change to this plan, TE 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.

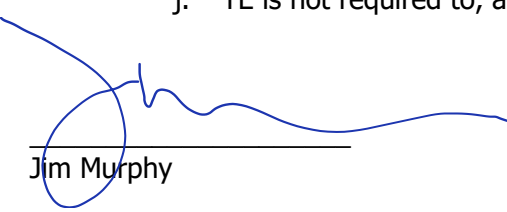
Certification of Jim Murphy

I, Jim Murphy, CEO of Telecom Evolutions LLC ("TE") do hereby certify, under penalty of perjury, the following:

- a. TE is not required to implement STIR/SHAKEN, due to its lack of control over the necessary infrastructure.
- b. TE's business name and primary address are as follows:

Telecom Evolutions, LLC
9221 Corbin Avenue Suite 155,
Northridge, CA 91324

- c. TE has no other business names in use.
- d. TE has not previously used any other business name.
- e. 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.
- f. The sole entity with 10% or more ownership in TE is Jim Murphy. TE has no parent companies, subsidiaries, or affiliates.
- g. TE's role in the call chain is that of a voice service provider with no STIR/SHAKEN implementation obligation.
- h. TE is not prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- i. TE has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- j. TE is not required to, and does not have, an Operator Code Number.



Jim Murphy