

Robocall Mitigation Plan - Updated 25th August, 2026

TELORCA LLC

16192 Coastal Highway,
Lewes, Delaware 19958

Contact Information

Mohammed Zabiulla

(Manager)

zabi@telorca.com

Overview

The FCC requires that all small 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. Telorca LL does not originate anycalls or serving end-users at the moment, but only serving as an intermediate carrier provider serving resellers.

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

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

Know Your Customer (“KYC”)

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

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

TELORCA’s KYC program involves obtaining specific subscriber information when payment is made for

services. This process includes collecting such information such as:

- physical business location;
- contact person(s);
- nature of the customer's business;
- customer listing in the RDM database, FC 499;
- customer Stir/Shaken certification if available.

Acceptable Use Policy ("AUP")

TELORCA maintains an AUP that subscribers must agree to before being permitted to use TELORCA'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 law;
- violating applicable industry accepted guidelines; and
- using TELORCA's service to engage in or in connection with fraudulent activities.

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

Monitoring

TELORCA works with its upstream carrier to detect a calling pattern consistent with illegal robocalls. If such a call is detected, TELORCA will identify the party that is using our network to originate those calls and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our network.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, TELORCA follows certain 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 behaviour;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.

Traceback

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robo-callers that use our service to originate calls. To allow for timely and comprehensive responses, TELORCA will devote sufficient resources to provide prompt and complete resources within 24 hours to any traceback requests.

Robocall Mitigation Program

We use software provided by VOS and CONNEXCS to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls.

Combining behavioural analytics, caller authentication and verification, our solution features:

Fraud Detection: Detection of high volume robocalling, spoofing and spam call activity.

Subscriber Notification: Caller ID Name override to warn subscribers of suspicious calls.

Call Blocking Support: Accurate identification enabling us to block fraudulent phone calls as per the TRACED Act (2019), plus numbers never issued by NECA, numbers identified by commercial switches as returning SIP codes indicating the numbers are not active, and other methods.

Business Number Verification: Register legitimate business numbers to prevent unintentional call blocking.

Caller ID Name Service: Easy integration of Caller ID name lookup service, including robocall mitigation with override to include original caller ID even when call is determined fraudulent.

In addition, we have implemented a Call Abuse Policy and have published the following policy to our web site, terms of use, and have notified our customers of the policy as copied below:

“Any call originated on the network is subject to inspection and investigation if the call is suspected of being fraudulent, abusive, or illegal. Calls meeting any of these criteria will be blocked. If these conditions are repeated, becoming excessive, the subscriber may be disconnected from the TELORCA network, may be subject to further investigation by the FCC for enforcement of the TRACED Act and the subscriber may be subject to fines and penalties imposed by the FCC or the jurisdictional court.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. TELORCA 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, TELORCA 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.

STIR/SHAKEN Assignment

We have secured our own our own Stir/Shaken certification. Most of the clients are signing their own calls. Unsigned calls are automatically rejected back by our switch. We have capabilities to reject calls that comes with "C- Attestation" or 'B-Attestation" if needed on our side. We do provide call signing with "A-Attestation" if the client is buying DIDs and using those as CLI for the traffic stream from us directly. In case client is using DIDs from other sources and providing the proof of their ownership, we provide the client with "B-Attestation" for the calls.