



Robocall Mitigation Program

Version 1.1



Table of Contents

1. Purpose	1
2. Certification Statement	1
3. Robocall Mitigation Program Overview	4
a. Customer Vetting and Onboarding Controls	4
b. Traffic Monitoring and Analytics.	4
c. Mitigation and Enforcement Actions.	4
d. Traceback Cooperation Commitment.	5
e. Record Retention.	5
4. STIR/SHAKEN Implementation Plan	5
5. Ongoing Review and Compliance	6
6. Authorized Representative	6



Revision History

Version	Date	Created By	Description
1.1	2026-02-28	Telna	



Company Name: Telecom North America Mobile Inc
Company Address: 3 Columbus Circle, Suite 1420, New York City, NY
Company Phone #: (415) 577-8338

1. Purpose

Pursuant to 47 C.F.R. § 64.6305 Telecom North America Mobile Inc submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This report describes the status of its implementation of STIR/SHAKEN and the practices and procedures Telecom North America Mobile Inc (hereinafter also referred to as “TELNA” or “the company”) has in place to mitigate illegal robocalls. The company may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time to respond to changes in its business, its capabilities and its needs.

Telecom North America Mobile Inc is a subsidiary of Telecom North America Inc. The company also operated under the name 3U Telecom Inc. The role the company plays in the network is as a Voice Service Provider (End User and Wholesale). TELNA has SS7 Voice, Data, Text, and VoLTE traffic on its network. It is registered with the STI-PA using 955F. [REDACTED]

Telecom North America, Inc. was acquired in stages between 2014 and 2018 by KNOWROAMING, Inc., a Canadian corporation based in Toronto, Ontario. On September 27th, 2019, KNOWROAMING, Inc. officially changed its name to TELNA, Inc. [REDACTED]

TELNA has fewer than 100,000 subscribers enabled for voice services and is therefore eligible for the STIR/SHAKEN implementation exemption for small carriers under 47 CFR § 64.6304. The company requires this extension to complete the implementation of the STIR/SHAKEN technology. At this time, TELNA is currently using [REDACTED] to sign our current subscriber calls, while actively working towards STIR/SHAKEN implementation in collaboration with [REDACTED] to acquire our own token. TELNA will update its certification within 10 days of any changes.

2. Certification Statement

TELNA hereby certifies that:

- TELNA follows the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

- This process includes the collection and review of entity-identifying information to confirm that the company has an authenticated relationship with the customer. The Company uses this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do. End users are not allowed to hide or change their caller IDs. They are limited to one active call at a time and it cannot last more than 60 minutes.
- TELNA also validates, when possible, that the entity has a legitimate right to use its asserted calling numbers. The Company uses this information to support the attestation level it assigns to calls that it originates for that customer.
- TELNA contractual provisions with customers prohibit them from initiating illegal robocalls. If the Company discovers a customer is initiating suspicious robocalls, it warns them to stop. If such traffic continues, then the Company terminates their service.
- TELNA requires that upstream providers have a reasonable Robocall Mitigation Plan, including a vetting process for their customers as well as their upstream providers, and that they use call analytics to identify suspicious traffic.
- Prior to installing services for new customers, the company takes the following measures to weed out end users that could potentially generate robocall traffic:
 - The Company uses a KYCs to confirm the following information for its customers:
 - Customer's identity by requiring USA REAL IDs or Passports
 - Customer's right to use the telephone number presented on calls
 - Service Address
 - When the customer is a business, TELNA also requires Business Incorporation Documents and verifies they have a reputation as a valid business that abides by the law.
- TELNA uses call analytics software provided by [REDACTED] to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls.
- All users are identified by SIM card. The Company will immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If the Company determines that the traffic was likely unlawful, then the company will warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then the company will terminate their service.
- TELNA will comply fully with all conditions set forth in the FCC'S Report and Order mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission's rules and policies more generally.
- TELNA has designated an individual as a dedicated point of contact for addressing traceback requests. RMD Contact is [REDACTED]. It either has provided the ITG with the contact information and business hours for those individuals, or will do so upon receipt of the first request from the ITG. See <https://www.ustelecom.org/the-industry-traceback-group-itg/for-providers/>. The Company will respond promptly to inquiries from the Industry Traceback Group (ITG) within 24 hours.



- If a pattern of questionable activity is detected TELNA will suspend service while investigating the situation. If it is discovered that the call was illegal, the customer may be suspended until the problem has been remedied. If they do not respond swiftly and appropriately, we will terminate their service. Requests from the ITG must be submitted in writing and include the following information:

Phone Number in Question
Phone Number Dialed
Date / Time Stamp:
Requestor's Name:
Requestor's Company Name:
Requestor's Title:
Requestor's phone number:
Requestor's e-mail:

- TELNA will provide valid law enforcement and regulatory agencies with the relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities, and implement mandated Robocall Mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls. The company will respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. The company will cooperate fully with such entities in investigating and stopping any illegal robocallers that use the Company's service to originate, carry, or process illegal robocalls. Requests from the valid agency must be submitted in writing and include the following information:

Law Enforcement Agency Name:
Agency Address:
Requestor's Name:
Requestor's Title:
Requestor's phone number:
Requestor's e-mail:

- TELNA performs the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call. The Company has not had any agency action or investigation due to suspected unlawful robocalling or investigations.
- TELNA is not subject, and has not ever been subject, to any Commission, Law Enforcement, or Regulatory Agency Action or investigation due to suspected unlawful robocalling or spoofing.

TELNA does not wish to publicize any private and/or classified information that has the potential to expose the Company to fraud and/or anti-competitive actions. Therefore, the Company will submit a

redacted version for the public site and requests that the FCC keep the unredacted version **CONFIDENTIAL**.

3. Robocall Mitigation Program Overview

TELNA has implemented a comprehensive robocall mitigation framework designed to prevent the origination of illegal robocalls and ensure rapid response to enforcement inquiries.

a. Customer Vetting and Onboarding Controls

TELNA applies reasonable and risk-based due diligence measures prior to onboarding customers, including:

- Know-Your-Customer (KYC) verification procedures
- Validation of corporate registration and beneficial ownership where applicable
- Review of the nature of the customer's business and intended traffic profile
- Screening against regulatory enforcement lists and known bad actors
- Contractual provisions prohibiting illegal robocalling and traffic pumping

Customers are required to certify compliance with applicable telecommunications laws and regulations as part of their service agreements.

b. Traffic Monitoring and Analytics.

TELNA automatically monitors traffic patterns across its network to detect and mitigate suspicious or unlawful activity using software analytics provided by [REDACTED]

[REDACTED] Monitoring measures include:

- Analysis of call volume patterns and spikes on a per user basis
- Review of answer-seizure ratios (ASR) and average call duration (ACD)
- Detection of high-volume short-duration call patterns
- Monitoring of complaint-driven triggers
- Identification of anomalous routing behavior

Where suspicious patterns are identified, TELNA investigates and may take immediate corrective action.

c. Mitigation and Enforcement Actions.

If illegal or suspicious robocall traffic is detected, TELNA may take the following actions:

- Immediate notification to the customer
- Temporary traffic suspension
- Blocking of specific call paths or number ranges
- Request for call detail records and traffic justification
- Termination of service for non-compliance
- Reporting to appropriate regulatory or enforcement authorities, when required

TELNA maintains internal escalation procedures to ensure timely decision-making and enforcement.

d. **Traceback Cooperation Commitment.**

TELNA maintains procedures to ensure full cooperation with traceback investigations.

TELNA commits to:

- Respond fully to all traceback requests from the FCC, law enforcement agencies, and the Industry Traceback Consortium.
- Provide accurate call detail records and routing information as required.
- Identify upstream and downstream providers associated with suspicious traffic.
- Take immediate steps to mitigate or terminate unlawful traffic identified through traceback efforts.

TELNA designates responsible companies to manage and respond to traceback inquiries to ensure compliance within required timelines.

e. **Record Retention.**

TELNA retains call detail records and relevant traffic data in accordance with regulatory requirements to support traceback investigations and internal compliance monitoring.

4. **STIR/SHAKEN Implementation Plan**

TELNA is in the process of implementing direct STIR/SHAKEN on its network in coordination with [REDACTED]. In the meantime, TELNA is using a third party as a supplier to terminate and sign calls on behalf of TELNA.

TELNA is currently:

- TELNA is using a third party as a supplier to terminate and sign calls on behalf of TELNA.



-
- Coordinating with [REDACTED] regarding certificate acquisition and operational readiness for its own NPA-NXX ranges.
 - Reviewing technical integration requirements.
 - Preparing network elements and processes necessary to support authentication and attestation.

TELNA intends to implement STIR/SHAKEN for its NPA-NXX ranges, as soon as technically and operationally feasible and will update its Robocall Mitigation Database filing accordingly.

5. Ongoing Review and Compliance

TELNA reviews its Robocall Mitigation Program periodically to ensure continued compliance with FCC regulations and evolving industry standards.

This program is subject to updates as regulatory requirements evolve or as STIR/SHAKEN implementation progresses.

6. Authorized Representative

I certify under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Company Name: Telecom North America Mobile Inc
Authorized Representative: Mr. Gregory Gundel Finger
Title: CEO
Date: 28-February-2026.