



Robocall Mitigation Plan (RMP)

Mobility Tech USA

April, 2026

1. Introduction

The Federal Communications Commission (FCC) requires all voice service providers to implement and maintain effective measures to prevent the origination, transmission, and processing of illegal robocall traffic within U.S. communications networks. These requirements are established in 47 C.F.R. § 64.6305, the Sixth Caller ID Authentication Report and Order (FCC 23-18, WC Docket No. 17-97, March 17, 2023), and subsequent FCC updates.

The FCC further requires all providers to certify in the Commission's Robocall Mitigation Database (RMD) whether they have fully implemented the STIR/SHAKEN caller-ID authentication framework and whether all calls they originate, carry, or process are subject to a compliant robocall mitigation program. Under 47 C.F.R. § 64.6305(a)(2), a provider's mitigation plan must "include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond within 24 hours to all traceback requests from the Commission, 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 transmit calls."

Mobility Tech USA, LLC ("MOBILITY") acknowledges these regulatory obligations and is committed to maintaining a secure, lawful, and compliant telecommunications environment. MOBILITY has adopted a comprehensive, multilayered compliance framework incorporating advanced technical safeguards, stringent customer-vetting protocols, and continuous traffic monitoring to prevent the origination or transmission of illegal robocall activity.

MOBILITY operates in multiple capacities depending on the business relationship and traffic type. Specifically, MOBILITY may act as a Voice Service Provider, Gateway Provider, or Intermediate Provider. Each role carries distinct regulatory obligations and risk profiles. Accordingly, MOBILITY has implemented a role-based mitigation structure that includes rigorous Know-Your-Customer (KYC) and Know-Your-Upstream-Provider (KYUP) procedures to verify customer identity, legitimacy, expected traffic characteristics, and risk level, with enhanced due diligence applied to high-risk customers, gateway traffic, and foreign sources. MOBILITY also provides complete responses to all Industry Traceback Group (ITG) inquiries within 24 hours, as required by the FCC.

This Robocall Mitigation Plan (RMP) outlines MOBILITY's affirmative and effective measures to prevent illegal robocall traffic across its network. It includes MOBILITY's commitment to apply STIR/SHAKEN caller-ID authentication to all SIP calls carrying a U.S. number, implement mandatory blocking where required, enforce Do-Not-Originate (DNO) protections, and maintain robust monitoring and mitigation procedures.

As required, MOBILITY will update its RMD filing within ten (10) business days of any change to covered information, including updates to this RMP.

Finally, MOBILITY acknowledges that its prior RMD certification was removed by Commission action (detail explanation is described below) and affirms that it has now adopted enhanced compliance safeguards and respectfully requests authorization from the Commission to reinstate its registration in the RMD.

2. Company Description

Mobility Tech USA, LLC (“MOBILITY”), established in 2020, is a U.S. based telecommunications provider specializing in wholesale and enterprise voice solutions, including international termination and VoIP services. Since its formation, the company has served global carriers and service providers by delivering reliable voice transport, high-quality routing, and compliant access to U.S. communications networks. MOBILITY operates with a strong commitment to regulatory compliance, network integrity, and secure traffic management within the U.S. and international telecom ecosystem.

Principals: Jorge Reyes Montoya

3. STIR/SHAKEN Call Authentication

MOBILITY has fully implemented STIR/SHAKEN protocols for all SIP calls eligible for authentication that carry U.S. NANP numbers. The company is properly registered within the STIR/SHAKEN governance framework and complies with all applicable STIR/SHAKEN requirements. MOBILITY signs calls, in accordance with industry standards to promote caller ID authentication and trust in the U.S. voice ecosystem.

4. Know Your Customer (KYC) and Customer Vetting Practices

KYC Protocol

MOBILITY maintains a Know Your Customer (KYC) process designed to verify the identity, legitimacy, and traffic intent of every upstream provider, with enhanced due diligence applied based on the type of service MOBILITY provides. These procedures ensure compliance with FCC rules, reduce the risk of illegal robocall activity, and align with industry best practices.

MOBILITY has developed a KYC process that collects essential identity and business information from every customer, including:

- Legal name and DBAs
- Jurisdiction of incorporation and business registration
- EIN or foreign tax ID
- Physical business address
- Website or online presence
- Primary contacts, including technical and compliance representatives;
- FCC FRN and Form 499 Filer ID (if applicable); and
- Description of service and traffic types (A2P, P2P, enterprise, call center, etc.).

Before activating service, MOBILITY validates the customer’s information and risk profile through multiple verification steps, including:

- Reviewing the customer’s website, online presence, and physical address;

- Confirming corporate existence, legal status, and ownership details;
- Verifying the customer's listing in the FCC RMD

MOBILITY retains all completed KYC forms and supporting documentation in accordance with its internal recordkeeping and audit policies.

Role-Specific Risk Assessment

Because regulatory obligations and exposure to illegal robocall activity vary by role, MOBILITY applies different levels of due diligence, documentation requirements, and monitoring standards.

5. Mandatory Blocking Following Commission Notification

MOBILITY will immediately block any traffic or source that the FCC identifies as originating illegal robocalls, consistent with applicable rules and enforcement actions.

6. Proactive Network Monitoring and Call Filtering

MOBILITY continuously monitors its network and traffic patterns to detect, prevent, and mitigate potential illegal robocall or spoofing activity. As part of this process, the company regularly reviews Call Detail Records (CDRs) and key performance indicators to identify unusual or suspicious behavior, such as short-duration call spikes, abnormal Answer-Seizure Ratios (ASR), irregular Average Call Duration (ACD), elevated Post-Dial Delay (PDD), or repetitive call bursts originating from single sources.

When illegal robocalling activity is suspected, or when the FCC, customers, or other authorities report such activity, MOBILITY immediately initiates an internal investigation to identify the responsible upstream provider or traffic source. Upon identification, MOBILITY takes prompt and appropriate corrective action, which may include blocking the implicated numbers or trunks pending further review and notifying the associated upstream providers to prevent continued transmission of illegal traffic.

MOBILITY continuously evaluates and enhances its monitoring thresholds, fraud-detection frameworks, and escalation protocols to ensure ongoing compliance with evolving FCC requirements.

7. Blocking Calls on Do Not Originate (DNO) List

MOBILITY maintains a Do-Not-Originate (DNO) list consisting of numbers that should never generate outbound traffic, including invalid or unassigned numbers, numbers designated as DNO by their rightful owners.

MOBILITY blocks numbers that have been identified through fraud and scam reports.

MOBILITY utilizes SIP Code 603+ as the standardized response for analytics-based call blocking, ensuring proper signaling, compliance with applicable FCC requirements, and transparency across the network.

8. Emergency Call Handling and 911 Safeguards

MOBILITY affirms that, in accordance with FCC rules, it won't block any emergency calls placed to 911. MOBILITY also takes all reasonable measures to ensure that calls

originating from Public Safety Answering Points (PSAPs) and other government emergency numbers are not blocked. These protections are incorporated into MOBILITY's call-blocking policies and monitoring systems to ensure uninterrupted access to emergency services

9. Caller ID & Number Authorization

When MOBILITY customer is the end user that originates, the call is permitted to display only those Caller ID numbers that have been legitimately assigned to them by MOBILITY or numbers for which they have documented authorization. Any unauthorized manipulation or falsification of Caller ID information is strictly prohibited and will result in immediate service suspension or termination.

10. Contractual Provisions to Prevent Illegal Robocalling

MOBILITY maintains strict contractual requirements designed to prevent the use of its network for illegal robocalls or any other unlawful activity. All customers must sign a Master Service Agreement ("MSA") and agree to MOBILITY's Acceptable Use Policy ("AUP") prior to activation. These agreements prohibit unlawful, fraudulent, or abusive calling practices and grant MOBILITY the authority to immediately suspend or terminate service if prohibited activity is detected.

The MSA identifies illegal robocalling, caller ID spoofing, and other violations of federal or international law as material breaches and requires customers to comply with all applicable FCC regulations. Customers must also meet ongoing cooperation and transparency obligations, including:

- Prohibiting the use of MOBILITY's services for any unlawful, fraudulent, abusive, or deceptive purpose, including illegal robocalling, caller ID spoofing, or the transmission of traffic that violates U.S. or international law.
- Fully cooperating with MOBILITY in responding to ITG and law-enforcement traceback requests within 24 hours, including providing accurate and timely information regarding upstream providers and traffic sources.

11. Traceback Requests Process

MOBILITY commits to respond within 24 hours to traceback requests from the FCC, law enforcement and the ITG in all traceback investigations.

- All traceback requests are acknowledged and responded to within 24 hours of receipt.
- Internal tickets are created for every traceback request, and customers involved in the call chain are contacted for investigation.
- If illegal traffic is confirmed, the affected customer's account is immediately suspended pending resolution.
- MOBILITY retains traceback records and communications for at least two years.
- MOBILITY has designated a dedicated point of contact for addressing requests from other VSP, ITG or any other government entity related to

suspicious Traffic. This person will oversee all matters regarding robocall mitigation action:

MOBILITY Point of Contact:

Name:	Ray Lacouture
Title:	NOC
Email:	noc@mobilitytechusa.com
Phone:	+1 (786) 327-7139

12. Accepting Traffic from Providers in the RMD

As required, MOBILITY will accept U.S.-bound traffic only from upstream providers that are actively listed in the FCC's RMD.

13. Employee Training

MOBILITY trains all staff responsible for network operations, traffic monitoring, fraud controls, and traceback response on FCC robocall mitigation requirements. These employees receive and must stay familiar with the procedures outlined in this Robocall Mitigation Plan (RMP).

14. Formal Commission, law enforcement, or regulatory agency action or investigation.

MOBILITY was subject to an enforcement action by the FCC Enforcement Bureau in connection with its Robocall Mitigation Database (RMD) certification. The Company was named in Public Notice DA-24-1235 (released December 10, 2024), which directed the Company to cure deficiencies in its RMD filing. The FCC determined that the Company's RMD filing was deficient due to incomplete or missing required information, including aspects of its robocall mitigation plan and certification. Following failure to timely cure the identified deficiencies, the FCC issued a final determination in Order DA-25-737 (released August 25, 2025), which removed the Company's RMD certification effective immediately. The matter is currently under review by the FCC Enforcement Bureau. MOBILITY remains committed to full compliance with FCC requirements and has implemented enhanced internal controls.