

March, 2026.



Robocall Mitigation Plan (RMP)

ICS International Carrier Services LLC

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 outlined in 47 C.F.R. § 64.6305 and in the Sixth Caller ID Authentication Report and Order (FCC 23-18, WC Docket No. 17-97, March 17, 2023).

ICS International Carrier Services LLC ("ICS") is committed to maintaining robust technical, procedural, and organizational controls to ensure compliance with FCC robocall mitigation rules.

To ensure compliance, ICS has implemented a robust Know Your Customer (KYC) protocol, real time network monitoring, and traceback cooperation protocols designed to significantly reduce the risk of originating or transmitting illegal robocall traffic over its network.

This Robocall Mitigation Plan (RMP) describes ICS's practices in accordance with the Commission's rules and serves as its official filing reference for the FCC Robocall Mitigation Database (RMD).

2. Company Description

ICS International Carrier Services LLC is a telecommunications carrier providing international and wholesale voice services, including call termination, routing, and interconnection with international and U.S.-based partners.

Principals: Elias Melky - CEO

3. STIR/SHAKEN Call Authentication

ICS has Fully Implemented STIR/SHAKEN (Secure Telephone Identity Revisited/Signature-based Handling of Asserted Information Using Tokens) protocols for all SIP calls that are eligible for authentication carrying U.S. NANP numbers.

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

During onboarding, each prospective customer is required to complete a KYC questionnaire and formally acknowledge that its use of ICS's services is subject to a robust legal and regulatory regime governing outbound calling and voice traffic practices.

The KYC questionnaire collects essential identity and business information, including:

- Legal name, DBAs, and corporate structure;
- Jurisdiction of incorporation and business registration or license number;
- Tax or VAT identification number;
- Physical business address and website;
- Primary contacts, including technical and compliance representatives;
- FCC FRN and Form 499 Filer ID (if applicable); and
- Description of service use cases and traffic types (A2P, P2P, enterprise, call center, etc.).

Before activating service, ICS 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 Robocall Mitigation Database (RMD)

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

As part of onboarding, ICS also includes a Robocall Compliance Acknowledgment in its KYC form. Each customer must review and sign this acknowledgment before activation. By signing, the customer certifies that it:

- Complies with all applicable U.S. laws and FCC rules prohibiting illegal robocalls and caller-ID spoofing;
- Acknowledges and cooperates with the Industry Traceback Group (ITG) and its procedures;
- Agrees to respond promptly to traceback requests; and
- Will take effective measures to identify, investigate, and mitigate any suspected unlawful traffic on its network.

These measures ensure that only legitimate, verified, and compliant customers are granted access to ICS's network, thereby reducing the risk of illegal robocall.

5. Mandatory Blocking Following Commission Notification

In compliance with 47 C.F.R. § 64.1200(n)(5), ICS will immediately block any traffic or source identified by the FCC as originating illegal robocalls.

6. Proactive Network Monitoring, Call Filtering, and Blocking

ICS continuously monitors its network and traffic patterns to detect, prevent, and mitigate any potential illegal robocall or spoofing activity. The company regularly reviews Call Detail Records (CDRs) and network analytics to identify unusual or suspicious trends, such as short-duration calls, abnormal Answer-Seizure Ratios (ASR), Average Call Duration (ACD), Post-Dial Delay (PDD), or repetitive call bursts from single sources.

ICS maintains and enforces a reasonable Do-Not-Originate (DNO) list as part of its robocall mitigation program. The DNO list includes telephone numbers that should never originate outbound calls, such as invalid, unallocated, unused, or inbound-only numbers, as well as numbers for which subscribers or authorized entities have requested that outbound calling be blocked. ICS implements technical controls to prevent calls from appearing to originate from numbers on the DNO list and blocks such calls when detected.

When illegal robocalling activity is suspected or reported by the FCC, partners or other relevant authorities, ICS immediately initiates an internal investigation to identify the responsible customer or upstream provider.

Upon identification, ICS takes prompt and appropriate corrective action, which may include blocking the implicated numbers, trunks, or routes pending investigation and notifying the associated upstream providers to prevent further transmission of the illegal traffic

7. Traceback Requests Process

ICS 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.
- ICS retains traceback records and communications for at least two years.

Traceback Request Point of Contact:

- Name: Elias Melky
- Title: CEO
- Email: elias.melki@ics-voice.net
- Phone: +1 312-358-2272

8. RMD Registration and RMP Updates

As required ICS will update its RMD filing within ten (10) business days of any change to covered information, including its Robocall Mitigation Plan.

9. Accepting Traffic from Providers in the RMD

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

10. RMD certification

ICS affirms that no prior RMD certification has been removed by Commission action and that it has not been prohibited from filing in the RMD.