



December 18th, 2024

Introduction

Intelliverse operates as a voice service provider, originating calls on behalf of customers. As a critical participant in the call chain, we enforce stringent robocall mitigation protocols to ensure compliance and safeguard the integrity of telecommunications services.

Intelliverse Commitments

- **Rapid Response:** Fully responding within 24 hours to Traceback Requests from the Industry Traceback Group (ITG), and civil and criminal law enforcement agencies, cooperating fully in efforts to investigate and eliminate illegal robocalls.
- **Illegal Traffic Mitigation:** Taking decisive actions to mitigate illegal traffic upon receiving formal notifications from the FCC or other bodies.
- **Robocall Mitigation:** Enforcing comprehensive robocall mitigation prevent the origination and receipt of illegal calls on our network.
- **Customer Verification:** We only accept and deliver voice traffic from known customers through our custom applications, maintaining the legitimacy and operational integrity of clients.

Certification

- **Robocall Mitigation Certification:** Intelliverse certifies that all calls originating on our network are subjected to a robocall mitigation program that meets or exceeds the specified requirements.
- **Certification and Eligibility:** Intelliverse certifies that no prior certification has been removed by Commission action and that we are not prohibited from filing in the Robocall Mitigation Database (RMD). This certification confirms our ongoing compliance with FCC requirements.
- **STIR/SHAKEN Implementation:** Not Implemented Locally - Intelliverse numbers are issued from our upstream carrier partner who has verified KYC with us and they provide the STIR/SHAKEN signing on our calls.
- **Investigations and Compliance History:** Intelliverse certifies that neither the company nor its affiliated entities have been subject to any FCC or law enforcement investigations regarding illegal robocalling, spoofing, or deficiencies in our RMD certification within the past two years. Should any such issues arise in the future, we are committed to addressing them promptly and transparently.

STIR/SHAKEN Extensions and Exemptions

- We are eligible for and are taking STIR/SHAKEN implementation extension received under 47 CFR § 64.6304 because we have fewer than 100,000 voice subscriber lines.

- Unable to Obtain SPC Tokens – Providers that are unable to obtain the SPC tokens necessary to authenticate calls have an indefinite exemption from implementing STIR/SHAKEN until the provider is capable of obtaining a token.
- All the voice traffic that originates on our network is subject to the robocall mitigation plan described below.

Despite this extension, we are committed to achieving full STIR/SHAKEN compliance. To this end, we are actively:

- Working with our compliance partner to explore token acquisition requirements.
- Updating our infrastructure to enable native STIR/SHAKEN capabilities.
- Planning to implement a full solution by Q4 2025, subject to resource availability and regulatory updates.

This phased approach ensures that we remain proactive in mitigating illegal robocalls while adhering to regulatory guidelines.

Robocall Mitigation Plan

1. Prevention Measures for Illegal Robocalls (Voice Service Provider Role)
 - a. Conduct Know Your Customer (KYC) procedures, including verification of customer identity and business legitimacy. 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>)
 - b. Require customers to agree to acceptable use policies prohibiting illegal robocalls.
 - c. Monitor call patterns for indicators of illegal robocall activity, such as high call volumes with short duration or invalid call destinations.
2. Call Analytics Systems
 - a. Internal and Third-Party Solutions:
 - i. Utilize real-time call analytics tools to identify and block suspicious call traffic.
 - ii. Partner with reputable third-party vendors providing call analytics and robocall detection.
3. Upstream Provider Verification
 - a. Verify the identity and compliance of all upstream providers in our call chain.
 - b. Verify upstream providers certifying their compliance with robocall mitigation requirements via the RMD.
 - c. Monitor call traffic received from upstream providers for unusual patterns indicative of illegal robocalls.

David Godlewski - CEO

david.godlewski@intelliverse.com

Office: 770-663-5072

8000 Avalon Blvd Suite 100

Alpharetta, GA 30009