



February, 2026

Robocall Mitigation Plan

WMMN USA LLC

Pursuant to 47 C.F.R. § 64.6305 WMMN USA LLC. 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 WMMN USA LLC. (hereinafter also referred to as “company name abbreviation” 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.

WMMN USA LLC doesn’t have a parent company, affiliate or subsidiary.

WMMN USA LLC operates as a Voice Service Provider, Gateway Provider, and Non-Gateway Intermediate Provider.

1. Call Authentication

Our registered OCN is 023M and we have fully implemented STIR/SHAKEN (Secure Telephone Identity Revisited / Signature-based Handling of Asserted Information Using Tokens) protocols for all SIP calls eligible for authentication that carry U.S. NANP numbers. The company is fully registered and compliant with all applicable STIR/SHAKEN requirements.

2. Company Principals

Boruch Weiss – CEO

3. Network Monitoring and Proactive Blocking.

WMMN USA LLC utilizes the Veriswitch switching platform to support traffic monitoring, fraud detection, and enforcement controls as part of its robocall mitigation program. Through the Veriswitch platform, WMMN monitors traffic activity in real time and applies operational safeguards designed to identify and address potentially unlawful robocall traffic. These controls include:

- Monitoring traffic volumes, call patterns, and routing behavior for irregular or suspicious activity.
- Reviewing call performance indicators such as short-duration call patterns and abnormal traffic spikes.
- Enforcing call routing restrictions, customer-specific limits, and suspension controls when suspicious traffic is identified.
- Investigating traffic associated with invalid, spoofed, or unauthorized Caller ID presentation.

WMMN USA LLC's Network Operations team actively reviews network activity and investigates anomalous traffic patterns. When potentially illegal robocalling, spoofing, or fraudulent traffic is suspected, WMMN USA LLC promptly investigates the source and takes appropriate corrective action, which may include traffic blocking, customer suspension, or termination.

WMMN USA LLC utilizes Do-Not-Originate (DNO) lists as part of its robocall mitigation controls. These lists are incorporated into the Company's traffic monitoring and filtering processes to prevent the origination or transmission of calls using invalid, unallocated, or unauthorized telephone numbers. WMMN USA LLC 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

WMMN USA LLC will promptly investigate and block illegal traffic upon receiving a notice from the Commission's Enforcement Bureau

Calls bearing valid STIR/SHAKEN authentication are passed without alteration, consistent with FCC guidance.

In accordance with FCC rules, WMMN USA LLC does not block emergency calls placed to 911 and takes reasonable measures to avoid blocking calls originating from Public Safety Answering Points (PSAPs) and other authorized government emergency numbers, consistent with 47 C.F.R. § 64.1200(k)(9).

4. General Terms and Conditions and Acceptable Use Policy

WMMN USA LLC prohibits customers from originating unlawful, fraudulent, or otherwise illegal traffic through its network, including unlawful robocalls or calls using false, misleading, or invalid caller identification information.

Pursuant to its Terms and Conditions and Acceptable Use Policy ("AUP"), WMMN USA LLC reserves the right to investigate, restrict, suspend, or terminate services where it determines that a customer is engaged in fraudulent, unlawful, or abusive calling activity.

WMMN USA LLC's Robocall Mitigation Program (RMP) includes ongoing monitoring, enforcement mechanisms, and compliance oversight designed to detect and prevent the transmission of unlawful traffic over its network.

5. Customer Vetting and KYC protocols

WMMN USA LLC maintains a review process for its upstream providers. WMMN USA LLC confirms that its upstream providers are registered in the FCC's Robocall Mitigation Database and does not accept traffic from unregistered providers. WMMN also requires upstream partners to maintain reasonable robocall mitigation programs, including customer vetting and traffic monitoring controls.

WMMN USA LLC conducts Know-Your-Customer (KYC) procedures prior to activating service for new customers. This review includes verification of customer identity, service address, business legitimacy (where applicable), and the nature of traffic. Business customers may be required to provide incorporation documents and related information to confirm lawful operations.

6. Traceback Process and Best Practices

WMMN USA LLC follows established industry protocols to address and respond to traceback requests in full compliance with 47 C.F.R. § 64.6305(a)(2), which requires providers to respond within 24 hours to traceback requests from the FCC, law enforcement agencies, and the Industry Traceback Group (ITG).

WMMN USA LLC 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.

Dedicated Point of Contact: The Company has designated the following individual as its Robocall Mitigation Database (RMD) and Traceback point of contact:

Name: Charlie Springall

Email: charlie.springall@wmmn.io