

Netvoice Solutions, LLC.

Robocall Mitigation Plan

January, 2026

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 set forth in 47 C.F.R. § 64.6305 and further detailed in the Sixth Caller ID Authentication Report and Order (WC Docket No. 17-97).

Pursuant to these rules, voice service providers must file a Robocall Mitigation Plan (“RMP”) and certification in the FCC’s Robocall Mitigation Database (“RMD”), indicating whether they have fully implemented the STIR/SHAKEN framework and certifying that any calls they originate, carry, or process are subject to an effective robocall mitigation program.

In accordance with 47 C.F.R. § 64.6305(a)(2), Netvoice Solutions RMP describes reasonable and effective measures to prevent illegal robocalls and affirms Netvoice Solutions commitment to respond within 24 hours to traceback requests from the FCC, law enforcement, and the Industry Traceback Group (“ITG”), and to cooperate fully in investigations of suspected unlawful robocall activity.

This RMP also outlines Netvoice Solutions Know Your Customer (KYC) procedures, as well as the analytic tools and third-party services used to detect, monitor, and mitigate potentially illegal traffic. Netvoice Solutions will update its RMD filing within ten (10) business days of any material change to the information provided.

Finally, NETVOICE SOLUTIONS affirms that any prior certification filed in the RMD has not been removed or revoked by Commission action and that NETVOICE SOLUTIONS is not prohibited from filing or maintaining certification in the RMD.

1. Stir-Shaken Implementation

NETVOICE SOLUTIONS has fully implemented the STIR/SHAKEN authentication framework on its network via upstream carrier implementation of STIR/SHAKEN.

2. Traceback Requests

NETVOICE SOLUTIONS will cooperate with the FCC, law enforcement and the ITG on all traceback requests and investigations. All traceback requests will be responded to within a 24-hour window. In addition to the automated traceback tickets generated by the ITG, NETVOICE SOLUTIONS will also open internal tickets with any customer/upstream carriers identified in the traceback.

All customers/upstream carriers must respond to traceback requests within the 24-hour window or face immediate account suspension.

Traceback Request Single Point of Contact:

Name: Robert Brown

Title: Owner

Email Address: nbrown@netvoicecloud.com

3. Customer Vetting Practices

In an effort to minimize or prevent illegal robocalls from traversing our network, NETVOICE SOLUTIONS will use its best practices to vet the identity of all of its customers/upstream carriers. NETVOICE SOLUTIONS attempts to confirm the identity of its potential customers by collecting KYC information such as physical customer location, billing address, state or province, country, year of incorporation, contact person(s), federal tax ID.

In addition to vetting the identity of potential customers, NETVOICE SOLUTIONS also collects the following information regarding:

- The nature of the customer's business.

4. Network Monitoring, Call Filtering and Blocking

NETVOICE SOLUTIONS monitors and reviews calls traversing our network and are audited regularly.

- NETVOICE SOLUTIONS uses Block lists to input originating or terminating numbers that appear in carrier tickets to prevent continuing abuse.
- NETVOICE SOLUTIONS uses carrier Global block lists maintained by the platform provider that include originating or terminating numbers, and media IP addresses that have been identified in ITG tracebacks and FCC enforcement actions.

NETVOICE SOLUTIONS monitors the usage of its network and examines call detail records (CDRs) for the purpose of detecting suspicious call activity and/or calling patterns. When we detect or are notified of suspected illegal robocalling or spoofing, we seek to immediately identify the customer carrier routing those calls so that we may take the appropriate action. The actions taken can include but are not limited to blocking the originating and terminating numbers pending investigation, immediately notifying the upstream carrier routing the calls of the issue and verifying the amount of traffic being received from our customer's client(s).

5. Mandatory Blocking Following Commission Notification

In accordance with FCC robocall mitigation rules, NETVOICE SOLUTIONS will promptly investigate and block any illegal traffic upon receiving a Notice of Suspected Illegal Traffic from the FCC's Enforcement Bureau.

6. Only Accepting Traffic from Providers in the RMD

In accordance with 47 C.F.R § 64.6305(e)(1), NETVOICE SOLUTIONS only accepts calls from Providers listed in the RMD via upstream carriers.

7. Contractual Provisions to Mitigate Illegal Robocalls and Acceptable Use Policy (AUP).

NETVOICE SOLUTIONS requires all customers to execute a Master Service Agreement ("MSA") that obligates compliance with all applicable federal, state, and international telecommunications laws and regulations, including those related to robocalls, caller ID authentication, and consumer protection.

NETVOICE SOLUTIONS prohibits the use of its services for any unlawful, fraudulent, abusive, or deceptive activity, including illegal robocalls, caller ID spoofing, or other non-compliant traffic, as further described in its Acceptable Use Policy ("AUP").

Pursuant to its MSA and AUP, NETVOICE SOLUTIONS may suspend or terminate services, without prior notice, where necessary to address policy violations, suspected fraud, regulatory compliance obligations, or to protect network integrity.