

Nuwave Communications Robocall Mitigation Plan

Date: 05/12/2025

1. Overview

Nuwave Communications, Inc. (“Nuwave”) has registered with the Robocall Mitigation Database and has fully implemented STIR/SHAKEN across the entire VOIP based network. Nuwave does not have TDM in its network, therefore STIR/SHAKEN has been fully implemented.

Nuwave operates a 24/7 telephony fraud monitoring team who receive real-time alerts from the fraud monitoring systems, and investigate and intervene as needed, including by blocking outbound calls if this is determined to be necessary.

The Robocall and additional fraud mitigation methods used by Nuwave are summarized below in Section 2.

2. Nuwave’s Robocall Mitigation Program:

Nuwave has deployed the STIR/SHAKEN caller ID authentication framework in its entire network. The following sets forth the specific reasonable steps Nuwave’s has taken to avoid originating illegal robocall traffic as part of our robocall and fraud mitigation program:

a) Call Analytics / Robocall Monitoring and Blocking:

As part of its robocall mitigation program, Nuwave currently leverages Transnexus NexOSS software (Nuwave’s third party analytics vendor) which monitors Robo Calling Patterns, high-volume voice network traffic and industry reputation scoring to detect robocalling patterns and identify high industry reputation scored calls. For both inbound and outbound calling through the Nuwave network (any call traversing the Nuwave network) and calls that match the aforementioned patterns or scoring will get blocked to SIP 603. Nuwave will also block any calls into the network that do not have an Identity header within the SIP Invite or fail verification through the STIR/SHAKEN framework.

i) Authentication/Signing of Nuwave Originated Traffic:

Nuwave has also implemented its STIR / SHAKEN caller ID authentication framework platform utilizing Ribbon’s Stir-Shaken Identity Hub (Nuwave’s third party-analytics vendor) enables

Robocall mitigation through: (i) the use of **authentication/signing (identify headers)** of SIP calls that originate from Nuwave subscribers and which will be sent for termination to PSTN where such identify headers are included in the outgoing invite for signed calls; and (ii) the ability to block/mitigate Robocalls automatically if the Nuwave network detects malicious patterns and also block calls with the outbound shield database (maintained by Transnexus NexOSS) if the following criteria is met :

Calling Party:

- Call has no CPN (calling party number) in From or PAI header
- There is a high reputation score attached to the calling party number
- From number with too few digits
- From number with too many digits
- CPN is within number blocks that have not been assigned by the Number Pooling Administrator for use by any carrier
- CPN is using an unassigned area code.
- Call meets Robo Calling Patterns
- No IDH in the ingress Invite
- IDH cannot be verified against STIR/SHAKEN framework

The outbound Shield database also contains a Nuwave curated list of high-risk calling numbers. Data sources include the FCC complaint database, and the Do Not Originate (DNO) database from the US Telecom Traceback Group. The outbound Shield database is maintained by Nuwave and updated hourly automatically.

ii) Verification of PSTN Originated Traffic:

As a further part of Nuwave's implementation of the STIR / SHAKEN utilizing Ribbon Identity Hub and caller ID authentication framework requirements, Nuwave further implements Robocall mitigation for the verification of PSTN originated voice calls through: (i) the verification of PSTN origination (inbound) voice traffic; and (ii) the ability to block/mitigate Robocalls.

Nuwave verifies every call that is sent into the network if a IDH (Identity header) is present and if not will block the call, and if the Identity header cannot be verified through the STIR/SHAKEN framework the call will also be blocked. In addition, Nuwave has automatic blocking of inbound SPAM and Robocalling to the Nuwave customers based on reputation scoring and Robo Calling

pattern thresholds and if the calling party meets the reputation score or Robo Calling pattern threshold, the call will get blocked with a SIP 603 decline.

For Inbound calls, Nuwave also uses the Shield database to block calls when these conditions are met:

Calling Party:

- Call has no CPN (calling party number) in From or PAI header
- There is a high reputation score attached to the calling party number
- From number with too few digits
- From number with too many digits
- CPN is within number blocks that have not been assigned by the Number Pooling Administrator for use by any carrier
- CPN is using an unassigned area code.
- Call meets Robo Calling Patterns
- No IDH in the ingress Invite
- IDH cannot be verified against STIR/SHAKEN framework

The inbound Shield database also contains a Nuwave curated list of high-risk calling numbers. Data sources include the FCC complaint database, and the Do Not Originate (DNO) database from the US Telecom Traceback Group. The inbound Shield database is maintained by Nuwave and updated hourly automatically.

b) Know Your Customer and Upstream Providers

Nuwave exercises due diligence with our upstream customers and upstream providers to help ensure that the type of traffic generated is in compliance with regulatory requirements and that relevant information regarding the end customers and upstream providers is known so that Nuwave is not used to transit illegal traffic and/or be able to remediate if identified.

c) Traceback Cooperation:

Nuwave is committed to promptly respond to all traceback requests from the Commission, law enforcement and the US Telecom ITG (Industry Traceback Group) and will cooperate and assist with such entities in investigating and stopping any illegal Robocallers that use our service to originate calls.

3. Principles and Parent Companies

Pursuant to paragraph 46 of the Sixth Caller ID Authentication Report and Order (FCC 23-18 adopted on March 16, 2023), Nuwave Communications, Inc. provides the following information regarding our principals, affiliates, subsidiaries, and parent companies:

- **Parent Company: Nuwave Communications, Inc.** – a US (Nevada) Corporation which is a domestic US entity owned by its principals Shawn Simms (US Citizen) and Mark Bunnell (US Citizen).
- **Subsidiary: Nuwave Communications (Canada) Limited** - a Canadian Corporation which is 100% owned by Nuwave Communications, Inc.
- **Subsidiary: Nuwave Communications Limited** - a UK Private Limited Company which is 100% owned by Nuwave Communications, Inc.
- **Subsidiary: Nuwave Communications (Australia) Pty Ltd** - an Australian Private Limited Company which is 100% owned by Nuwave Communications, Inc.
- **Subsidiary: Nuwave Cloud Services (Ireland) Limited** - an Ireland Private Limited Company which is 100% owned by Nuwave Communications, Inc.