

Robo Call Mitigation Plan

Netmaker Communications LLC (RMD File Number: RMD0007475), in partnership with our SIP Trunk provider, Bandwidth.com, Inc., supports STIR/SHAKEN and Robo Call Mitigation Compliance with a three-point support plan. A description and details of the Netmaker Communications network compliance approach are as follows:

Principles of Robo Calls and Compliance:

1. **Prevention:** Netmaker Communications, in coordination with our SIP trunk partner Bandwidth.com, is working vigorously to prevent unlawful robocalls originating from our network. We have implemented a stringent screening process that prevents companies with potentially fraudulent robocalling traffic from becoming customers. We have also informed and empowered our customers with the information they need to identify these unlawful calls as defined by the FCC.
2. **Detection:** Netmaker Communications/Bandwidth has an extensive fraud-mitigation team dedicated to identifying and analyzing potential robocall campaigns on our network and determining whether they are lawful. In alignment with the FCC rules, Bandwidth is augmenting its robocall detection technology to identify and block unlawful robocalls from traversing our network.
3. **Mitigation:** When an illegal robocall campaign is identified, Bandwidth executes several measures to block all existing and future calls associated with the unlawful campaign. We have developed call-blocking tools that prevent calls with specific unlawful ANI/'FROM' TN characteristics from traversing the Bandwidth network. Bandwidth personnel regularly analyze network traffic, search for illegal robocall campaigns, and utilize our call-blocking tools when appropriate. We work diligently with our customers to stop all detected unlawful robocall campaigns and actively communicate with those customers who may be in the path of such a campaign.

Working with our SIP trunk partner, Bandwidth.com, we identify and mitigate fraud by identifying bad actors utilizing invalid robocall systems to terminate unwanted, unlawful, and fraudulent calling.

There are multiple methods of identifying these types of calls. Within our network, we have decided the best way to support Robo Call Mitigation is through a process of identifying, scrubbing, and tracking these types of calls to treat them appropriately in adherence to the FCC mandate for Robo Call and STIR/SHAKEN Compliance.

Methods to Identify, Scrub, and Treat Robo Call Campaigns

1. Unallocated NPA-NXX-XXXX—Once a call comes into the Netmaker Communications/Bandwidth network, a scrub against the North America Numbering Plan provides the LERG database to verify the validity of the incoming calling number ID.
2. Invalid Number formats will be identified, tracked, and treated according to the behaviors of the calling party.

3. Invalid Packet formatting—if a packet is sent to the Netmaker Communications/Bandwidth network in a non-compliant format or order, the call will be blocked and treated based on its invalid formatting.
4. Invalid Alpha Numeric strings will be dropped or blocked based on the number of times those formats are sent to the Netmaker Communications/Bandwidth network.

Additionally, to prevent these types of fraudulent calls from making it to the network, advanced services and network features are deployed within our network environment.

Netmaker Communications continuously monitors network usage and call detail records (CDRs) to identify suspicious activity and patterns indicative of illegal robocalling:

- Netmaker Communications provides monthly call reports based on CDR to customers and part of these services we monitor the report metrics for unusual traffic volume, short call durations, sequential dialing patterns, calls to do-not-call registries, and invalid numbers to identify potential patterns of abuse.
- The Netmaker Communication Network Operations Center (NOC) actively monitors session boarder controllers looking for patterns associated with robocalling (unusual traffic volume, short call durations, sequential dialing patterns, calls to do-not-call registries, and invalid numbers) and implements a “denylist” on our network of Direct Inward Dial (DID) 10-digit numbers known be associated with spam or robocalls.
- Netmaker Communication takes immediate action upon detecting potential robocalls, including traceback investigations, customer verification, network termination, and notifying law enforcement authorities where appropriate. Additionally, Netmaker Communications is fully committed to responding to traceback requests within 24-hours.
- Respond to customer requests to actively denylist DID 10-digit numbers ensuring they do not receive inbound calls from those numbers.
- Netmaker Communications ensures all egress calls are validated as previously described before being sent to our SIP Trunk provider (e.g., Bandwidth.com). Netmaker Communications coordinates with Bandwidth.com to revalidate all SIP calls are associated with valid numbers assigned to Netmaker Communications and sign calls on our behalf.

Traffic Cost anomalies—for example, non-tariffed local calling—are rated for long-distance calling based on the originator's calling location.

Using SPAM filters and monitoring the use of URL Shorteners within a packet prevents Robo Calling and Fraudulent Calling bad actors from disguising their calling packet to carrier networks. We also monitor high-cost, high-fraud areas.

Lastly, engaging in partnerships with industry-setting teams ensures we are on the front line in setting standards and rules that govern these types of behavior.

Examples of Network Teams include, but not limited to:



NETMAKER COMMUNICATIONS

- SIP Forum Working Groups
- STIR/SHAKEN FCC Public Working Groups
- Fraud Control Associations Groups

Netmaker Communications' Growth Strategy

The next stage for the Netmaker Communications Network is to migrate to a Class 5 telephone switching service delivery platform. Today, we provide managed telecommunications services through our network partners, including Bandwith.com. By establishing Netmaker Communications' own switching environment, services like Robo Calling Mitigation and STIR/SHAKEN compliance will exist natively within the Netmaker Communications VOIP switching platform. This plan will be updated and refiled at that time.

Netmaker Communications will enforce and provide these services—along with others—by utilizing the same core principles implemented via our network partners today. Netmaker Communications will continue to support the high level of network integrity through prevention, detection, and support for calling-mitigation services that will make for seamless customer network integration and superior customer networking support.

Points of Contact:

Business Contact:

Jon Marcy
President & CEO
Netmaker Communications LLC
2654 Valley Ave., Suite J
Winchester, VA 22601
Ph: 540-431-4901 Ext. 11

Traceback Request Single Point of Contact:

Lee Curling
VP Engineering
lee.curling@ucnetmaker.net
540-431-4901 Ext. 21

Robocall Mitigation Single Point of Contact:

Lee Curling
VP Engineering
lee.curling@ucnetmaker.net
540-431-4901 Ext. 21

