

NEORACOM LLC



Pursuant to 47 C.F.R. § 64.6305 NEORACOM 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 NEORACOM 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.

NEORACOM LLC is an not an Affiliate, subsidiary or parent company of any company. The company has not ever been sold or acquired by another company .The role the company plays in the network is Voice Service Provider (End User) on its network. Neoracom LLC is registered with ITG iconectiv STI-PA approved providers list; our OCN number of 185M and PeeringHub is our Certificate Authority Holder. The Officers of the company are: Warner Baez.

NEORACOM LLC is judiciously working to prevent unlawful robocalls from originating on its network and in the meantime NEORACOM LLC. has implemented the following robocall mitigation plan to address unlawful robocall traffic.

NEORACOM LLC is judiciously working to prevent unlawful robocalls from originating on its network and has implemented the following robocall mitigation plan to address unlawful robocall traffic.

Automatic Number Identification Management: NEORACOM LLC shall block originating telephone numbers if identified based upon patterns of activity.

Proactive Blocking. NEORACOM LLC requests underlying carriers to block calls from phone numbers on Do-Not-Originate lists published by US Telecom and Neustar.

General Terms and Conditions. NEORACOM LLC prohibits customers from originating fraudulent calling using any fraudulent means, devices, or technologies. In fact, NEORACOM LLC’s end user Terms and Conditions permit NEORACOM LLC, without notice, to discontinue, block or suspend Services if necessary to prevent fraud, scams, tampering, schemes, false or invalid numbers. In short,

NEORACOM LLC shall block or suspend the service of any customers originating unlawful robocalls through NEORACOM LLC. NEORACOM LLC's RMP includes an increasing investment in resources over time to further strengthen adherence to compliance requirements by customers.

Acceptable Use Policy. NEORACOM LLC's Acceptable Use Policy ("AUP") also prohibits customers from utilizing the Service for any illegal, fraudulent, objectionable and/or unauthorized manner, reserving the sole and absolute right to deny, restrict or immediately suspend or terminate service if the use of the service by the 3 customer, or anyone having access to or using the service, either violates the NEORACOM LLC AUP or includes unlawful conduct.

Underlying Network Provider. NEORACOM LLC works with underlying providers and supports the benefit of deploying systems to detect potential robocall activity relying upon statistics such as average call duration, ASR, and call count carrier/consumer reports. NEORACOM LLC's regulatory compliance counsel confirms that NEORACOM LLC's underlying carriers maintain compliance with fully implemented STIR/SHAKEN protocols through the date of this RMP.

Traffic Reports and Industry Information. Reports generated by Call Detail Record and pattern trends, fraud information sharing through industry organizations, and third-party notifications and complaints, may identify potential unlawful robocalling. Although no evidence exists suggesting NEORACOM LLC in any way originates illegal robocall campaigns, in any instance where unlawful calling is identified, NEORACOM LLC maintains contractual ability to take any action it deems necessary to eliminate the fraudulent activity.

NEORACOM LLC has enforceable terms of use and/or an acceptable use policy noted in its contracts. These policies define the circumstances by which the company will deny, suspend, or terminate service to a customer. The company has a vetting and review process for upstream providers, that is, providers that send the company voice traffic that it terminates or transits to other providers.

NEORACOM LLC confirms that the upstream providers have a certification in the Robocall Mitigation Database. The company will not accept voice traffic from an unregistered provider. The Company has been informed of the upstream providers "Know-Your-Customer" guidelines and have provided them with the necessary KYC documentation they've requested that the company completes.

NEORACOM LLC follows the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

This process includes the collection and review of entity-identifying information to confirm that the company has an authenticated relationship with the customer. The Company uses this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

NEORACOM LLC also validates, when possible, that the entity has a legitimate right to use its asserted calling numbers. The Company uses this information to support the attestation level it assigns to calls that it originates for that customer.

NEORACOM LLC contractual provisions with customers prohibit them from initiating illegal robocalls. If the Company discovers a customer is initiating suspicious robocalls, it warns them to stop. If such traffic continues, then the Company terminates their service.

NEORACOM LLC requires that upstream providers have a reasonable Robocall Mitigation Plan, including a vetting process for their customers as well as their upstream providers, and that they use call analytics to identify suspicious traffic.

Prior to installing services for new customers, the company takes the following measures to weed out end users that could potentially generate robocall traffic:

The Company uses a KYCs to confirm the following information for its customers:

Customer’s identity

Customer’s right to use the telephone number presented on calls

Service Address

Credit History

Authentic and Legal Campaigns

When the customer is a business, NEORACOM LLC, also requires Business Incorporation Documents and verifies they have a reputation as a valid business that abides by the law.

NEORACOM LLC will comply fully with all conditions set forth in the FCC’S 2025 Report and Order mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission’s rules and policies more generally.

NEORACOM LLC has designated an individual as a dedicated point of contact for addressing traceback requests. **RMD Contact is Martin Hicks and martin@neoracom.com.** It either has provided the ITG with the contact information and business hours for those individuals, or will do so upon receipt of the first request from the ITG. See <https://www.ustelecom.org/the-industry-traceback-group-itg/for-providers/>. The Company will respond promptly to inquiries from the Industry Traceback Group (ITG) within 24 hours.

If a pattern of questionable activity is detected NEORACOM LLC.will require its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated.

Requests from the ITG must be submitted in writing and include the following information:

• Company Name: • Company Address:	• Phone Number in Question:	• Requestor’s Name: • Requestor’s Title: • Requestor’s phone number: • Requestor’s e-mail:
--	---	--

Requests from the valid agency must be submitted in writing and include the following information:

- Law Enforcement Agency Name:
- Agency Address:
- Requestor's Name:
- Requestor's Title:
- Requestor's phone number:
- Requestor's e-mail:



NEORACOM LLC

500 North Franklin Turnpike,
Ramsey, NJ, USA
443-713-1909
www.neoracom.com

