

Robocall Mitigation Plan

This robocall mitigation plan is for NEWCOM INC, with headquarters at 3600 RED RD STE 602A, MIRAMAR FL 33025.

We perform the following roles in the call chain:

- A voice service provider with a STIR/SHAKEN implementation obligation serving end-users

NEWCOM INC has not been prohibited from filing a certification in the Robocall Mitigation Database.

NEWCOM INC does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations.

NEWCOM INC uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls.

Know Your Customer

We follow 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 we have an authenticated relationship with the customer. We use 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.

We also validate, when possible, that the entity has a legitimate right to use its asserted calling numbers. We use this information to support the attestation level we assign to calls that we originate for that customer.

Our contractual provisions with customers prohibit them from initiating illegal robocalls. If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

Direct Customer Traffic Only

We maintain a strict policy that prohibits our customers from sending us traffic from third-party providers or acting as intermediate providers. All voice traffic must originate directly from our customers' networks, and we do not accept or transit traffic from upstream providers.

Customer Authentication and Direct Origination

Our contractual agreements explicitly prohibit customers from sending us voice traffic that originates from third parties or upstream providers. Each customer must certify that they are the originating source of all traffic sent to our network. This requirement is clearly outlined in our service agreements and is strictly enforced.

Call Path Integrity

Since we only accept direct customer-originated traffic, we maintain clear visibility of the complete call path. This direct relationship ensures we can effectively identify the source of all traffic and maintain accountability for call authentication and traffic patterns.

Enforcement

If we detect that a customer is sending us traffic from third parties or acting as an intermediate provider in violation of our policies, we:

1. Immediately notify the customer of the violation
2. May suspend service until the customer demonstrates compliance
3. May terminate service for repeated violations

Traceback

We respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. We cooperate fully with such entities in investigating and stopping any illegal robocallers that use our service to originate, carry, or process illegal robocalls.

Robocall Mitigation Program

We use call analytics software provided by TransNexus to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls.

The software provides detailed reporting to identify suspected illegal robocalls. The system alerts us if we process outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list.

We perform the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call.

We immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.

STIR/SHAKEN

We have registered with the STI-PA using OCN 636K. We have our own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA) that we use when authenticating calls we originate. We have implemented a STIR/SHAKEN solution supplied by TransNexus.