



Robocall Mitigation Plan

This robocall mitigation plan is for Nortex Communications, with headquarters at 205 N. Walnut St., Muenster, TX 76252.

Nortex Communications has taken the following reasonable steps to avoid the origination, carrying, and/or processing of illegal robocall traffic.

Use of Call Analytics Systems

Nortex Communications uses 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.

Affirmative, Effective Measures to Prevent New and Renewing Customers from Originating Illegal Calls

Nortex Communications 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 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.

If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

While requests for high-volume origination services are rare, Nortex exercises caution and extensively investigates new customers seeking access to such services.



[“Know-Your-Upstream Provider” Procedures](#)

Nortex Communications exercises due diligence before accepting traffic from an upstream provider in order to ensure that the provider is not using Nortex to carry or process a high volume of illegal traffic. It is Nortex’s policy to collect certain information from upstream providers, such as their physical business location, contact person(s), state or country of incorporation, federal tax ID (if applicable), and the nature of the provider’s business.

[Commitment to Responding to Traceback Requests](#)

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

[STIR/SHAKEN Implementation](#)

Nortex Communications has registered with the STI-PA using OCN 2116. 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.

Nortex still has portions of its network that are non-IP and cannot support STIR/SHAKEN. Therefore, Nortex continues to avail itself of the non-IP networks extension afforded under §64.6304(d) of the FCC’s rules for calls that originate or terminate on these portions of its network.