

Southeast Nebraska Communications, Inc. Robocall Mitigation Program

This Robocall Mitigation Plan describes the specific reasonable steps Southeast Nebraska Communications, Inc. (SNC) has taken to avoid the origination, carrying, or processing of illegal robocall traffic on its network.

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

SNC has a “know-your-customer” policy through which we exercise due diligence in ensuring that our services are not being used to originate illegal traffic. SNC uses best practices in vetting the identity of all of its voice service subscribers, both residential and business. Regarding business subscribers, SNC collects information such as their physical business location, contact person(s), state or country of incorporation, federal tax ID, and the general nature of their business.

Although SNC’s customers generally do not generate a high volume of calls, were we to receive a request for high-volume origination services, we would exercise caution and extensively investigate such customers before granting access to the services. In addition to collecting the information discussed above, this may also include a more stringent background check and possibly a site visit.

Furthermore, SNC customers are only able to originate calls from a number that identifies in the company’s switches as a number that has been assigned to them and that is directly managed by SNC (or obtained by SNC by an underlying partner). A call is dropped if a calling number that originates on our network is not owned by our customer and in use on our switch. This prevents SNC’s customers from engaging in malicious caller ID spoofing which greatly mitigates the likelihood of illegal robocalls originating on SNC’s network.

“Know-Your-Upstream Provider” Procedures

Currently, SNC receives traffic from only two upstream providers: Sinch and Windstream. SNC has longstanding relationships with both of these providers and we maintain awareness of the legitimacy of their call transmission services. SNC would exercise due diligence before accepting traffic from any new upstream provider as we seek to ensure that such providers are not using SNC to carry or process a high volume of illegal traffic. Specifically, SNC would collect information such as the upstream provider’s physical business location, contact person(s), state or country of incorporation, federal tax ID (if applicable), and the nature of their business. In addition, SNC would consider the inclusion of illegal robocall prevention language in contracts with any new upstream providers.

Use of Call Analytics Systems

SNC does not presently use any call analytics systems to identify and block inbound illegal robocall traffic.

SNC does monitor the usage of its network and examines call detail records (CDRs) on a recurring basis for the purpose of detecting unusual or suspicious call activity and/or calling patterns. Were SNC to identify activity or a pattern consistent with illegal robocalling, an investigation would be promptly undertaken. Were it determined that a customer was engaging in illegal call activity, SNC would take remedial action, which may include the suspension or termination of service, as appropriate.

Commitment to Respond to Traceback Requests

SNC commits to respond fully, within 24 hours, to all traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its services to originate, carry, or process illegal robocalls.