



RGTN USA Inc.

Robocall Mitigation Plan

This Robocall Mitigation Plan is submitted by RGTN USA, Inc. (“RGTN”) pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (FCC) which require all “voice service providers” to establish a robocall mitigation plan. Accordingly, this document sets forth RGTN’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network.

1. STIR-SHAKEN IMPLEMENTATION STATUS

As indicated in the FCC’s Robocall Mitigation Database, RGTN’s status with respect to STIR-SHAKEN implementation, RGTN has implemented the STIR/SHAKEN authentication framework on any portion of its network and all calls originating on its network are subject to the policies and procedures set forth in this Robocall Mitigation Plan which are intended to stop anyone from using RGTN’s service to originate illegal robocalls.

2. TRACEBACK REQUESTS

RGTN will promptly cooperate with the FCC, law enforcement, and industry groups on all traceback requests and investigations. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, RGTN will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from the FCC and law enforcement, and commits to fully responding to any traceback request received within 24 hours after receiving the same.

As part of its efforts to assist in the successful traceback of illegal robocalls, RGTN will include within its carrier interconnection and/or service agreements language requiring traceback cooperation on any voice service calls exchanged. In part, these related contract provisions will specify the need for parties to promptly identify the upstream provider from which a suspected illegal robocall entered its network or the customer of the service from which the call originated.

3. CUSTOMER VETTING PRACTICES

As a means of preventing or minimizing the origination of illegal robocalls through its voice services, RGTN will use best practices in vetting the identity of all of its voice service subscribers, including any entities that are purchasing RGTN’s services for resale.

The subscriber vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a service relationship. Generally, RGTN looks to confirm the identity of customers using its voice services through collecting information such as physical customer location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business.

Provider efforts to vet retail and business/commercial subscribers occur during the process of provisioning customer-requested services (for example in appropriately sizing the facilities to their claimed intended use), executing RGTN's required service agreements, and granting the customer the right to use telephone number resources. Commercial end-users, comprised of larger businesses with more complex service configurations, are generally recognized as presenting a higher risk of perpetrating illegal robocalls and thus those customers, at RGTN's discretion, may be subject to an additional review, including a more stringent background check and possibly a site visit.

Further, with respect to meeting existing obligations to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, RGTN:

- Utilizes service agreements and acceptable use policies as a means of preventing its new and existing subscribers from using their voice and broadband services in ways that would be in violation of local, state, or federal laws, or to engage in deceptive or fraudulent activity. These documents governing use of Provider-provided services include terms indicating specifically to all customers that their services should not be used for the purpose of making illegal robocalls, and RGTN reserves authority within its service agreements to suspend or terminate a subscriber's voice service for violating applicable service-related terms.
- Has established a routine process for monitoring of the usage and quality of its network facilities and conducts recurring and timely reviews of its call detail records (CDRs) to facilitate early identification of unusual or suspicious calling activity or patterns that may indicate use of the network for originating illegal robocalls. In those instances where RGTN identifies activity or a pattern consistent with illegal robocalls the customer will be contacted within twenty-four hours for further investigation and possible action regarding their subscribed to voice service.

4. TELEPHONE NUMBER VALIDATION PRACTICES

Telephone Number Validation refers to the confirmation of the customer or end-user right to use a telephone number in connection with their subscribed voice service(s). In accordance with industry best practices, RGTN has procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber of RGTN's services is permitted to use a telephone number as their caller identity if a number is directly managed by RGTN and/or obtained by RGTN via an underlying partner.

5. ONGOING ROBOCALL MITIGATION PRACTICES

RGTN monitors the usage of its network and examines call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and/or calling patterns. When network usage patterns consistent with illegal robocalls are detected or RGTN otherwise suspects illegal robocalling or spoofing is taking place on its network, it immediately seeks to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action.

The actions taken may include, but are not limited to: initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name; terminating the party's ability to originate, terminate, or route calls on RGTN's network; and providing notice to law enforcement authorities.

As part of its Plan to mitigate and prevent any originating robocalls on its network, RGTN is committed to early identification and investigation of possible robocalling situations. In monitoring usage of its network, particular attention is given to: (1) higher than normal subscriber traffic volume including large bursts of traffic in small timeframes or inconsistent volumes of traffic (spikes in usage); (2) originating calls of short duration and low call completion percentages; (3) originating calls with sequential called to number dialing patterns; (4) repeated calls made to do-not-call registry or invalid numbers; and (5) calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator.

Finally, RGTN will regularly audit and update its mitigation measures to adapt to evolving robocall tactics. And, RGTN will continually refine its processes and stay compliant with new regulations and technical standards.