

Syscom Technologies, Inc. d/b/a Syscom Business Technologies

Robocall Mitigation Plan

Last Revision: 4/26/2024

Last Revision by: Jeremy DeFrance

This Robocall Mitigation Plan is submitted by Syscom Technologies, Inc. d/b/a Syscom Business Technologies. 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”. This document sets forth the Provider’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. The Provider views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on its network and in addition to following these steps the Provider commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocaller's that may use its service to originate calls.

I. STIR-SHAKEN IMPLEMENTATION STATUS

As indicated in the FCC’s Robocall Mitigation Database, the Provider’s status with respect to STIR-SHAKEN implementation is as follows:

- Syscom Business Technologies utilizes the partner Bandwidth.com's services to implement STIR/SHAKEN technologies/procedures pursuant to the provisions of 47 CFR § 64.6304.
 - <https://bandwidth.com>
 - From <https://www.bandwidth.com/understanding-stir-shaken/>:
 - *"Bandwidth implemented STIR/SHAKEN in our network in December 2019 and we're currently signing over 4 billion calls each month. We've established interoperability with major carriers and other enhancements that will support our customers' compliance with STIR/SHAKEN."*
 - *"Consolidating your outbound calling and phone numbers with Bandwidth can simplify your compliance with STIR/SHAKEN. As a Bandwidth voice customer using our phone numbers, your calls are automatically signed with full or “A” attestation. This lowers the chance that your calls will be blocked by a terminating carrier."*

II. TRACEBACK REQUESTS

As noted above, the Provider will cooperate with the FCC, law enforcement and the (ITG) on all traceback requests and investigations. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, the Provider will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from the FCC, law enforcement and/or the ITG, and commits to fully responding to any traceback

request received within 24 hours after receiving the same. Within **Appendix A** to this Plan, the Provider identifies a single point of contact for receiving all traceback requests.

As part of its efforts to assist in the successful traceback of illegal robocalls, the Provider will going forward 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.

III. *CUSTOMER VETTING PRACTICES*

As a means of preventing or minimizing the origination of illegal robocalls through its voice services, the Provider will use best practices in vetting the identity of all of its voice service subscribers, whether a residential or business/commercial subscriber (including any entities that are purchasing the Provider'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, the Provider looks to confirm the identify 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 occurs during the process of provisioning customer requested services (for example in appropriately sizing the facilities to their claimed intended use), executing the Provider'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 the Provider'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, the Provider:

- Will utilize 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 the Provider reserves authority within its service agreements to suspend or terminate a subscriber's voice service for violating applicable service-related terms.

- Utilizes <https://www.bandwidth.com>'s processes for monitoring of the usage and quality of network facilities related to services 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 the Provider 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.

IV. 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 accord with industry best practices, the Provider has procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber of the Provider's services is permitted to use a telephone number as their caller identity if a number is directly managed by the Provider and/or obtained by the Provider via an underlying partner. These screening capabilities enable an automated and secure method of validating originating telephone numbers.

V. INTERNATIONAL CALL ORIGINATORS

The Provider is not currently an international voice services provider. If at any time the Provider does sell its services to customers which are international call originators using North American Numbering Plan resources it will familiarize itself with and develop best practices for fulling vetting such customers and performing telephone number validation on all international originated calls.

VI. KNOW YOUR UPSTREAM PROVIDER PROCEDURES

The Provider has longstanding relationships with upstream providers and maintains its awareness of the nature of their businesses and the legitimacy of their call transmission services. Further, the Provider, in the interest of providing the highest quality services to all of its voice service customers, is committed to taking those steps necessary to ensure that any upstream providers providing connectivity are equally committed to monitoring their networks and preventing their use for the transmission of illegal robocalls. This includes the use of robocall prevention language in any contracts that the Provider may directly have with any upstream provider entities.

VII. ONGOING ROBOCALL MITIGATION PRACTICES

As part of its Plan to mitigate and prevent any originating robocalls on its network, the Provider 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 time frames 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.

VIII. THIRD-PARTY ANALYTICS

The Provider also uses third-party call analytics to further assist and prevent the origination of illegal robocalls on its network. <https://www.bandwidth.com>

Appendix A

Traceback Request Single Point of Contact:

Name: Jeremy DeFrance

Title: COO

Phone Number: 231-486-5508

Email Address: jeremy@syscombusiness.com