

OrlanTech, Inc. - Robocall Mitigation Plan

This Robocall Mitigation Plan is submitted by OrlanTech, Inc. 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 robocalls that may use its service to originate calls.

I. PROVIDER ROLE

The Provider operates as a managed hosted PBX/voice service provider for business end users. The Provider installs and supports customer premises phone systems, servers and handsets, and administers the customer configuration and day-to-day operations. Voice traffic routes from customer endpoints through the Provider-managed voice gateway at the customer site, traverses the customer firewall, and is carried to/from the PSTN via the Provider’s interconnection with Bandwidth. The Provider controls provisioning, routing, access to the gateway and monitors traffic for anomalous patterns consistent with illegal robocalling and misuse

II. 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:

- The Provider hereby certifies that it has fully implemented the STIR/SKAKEN caller ID authentication framework across its entire Internet Protocol (IP)-based network, consistent with 47 CFR § 64.6301(a).
- Call authentication and signing are performed using the Provider’s own STIR/SKAKEN certificate (including where a third party performs the technical signing function) through Bandwidth’s hosted signing services and, where applicable, the Provider’s hosted PBX signing solution. The Provider assigns attestation levels based on its verification of the calling party and confirmation of the calling party’s authority to originate calls using the associated telephone number(s), consistent with applicable FCC rules, orders, and guidance.

III. 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 robocalls, 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 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.

The Provider will periodically review and maintain its robocall mitigation program and will update this plan and related filing information within 10 business days when material information changes, including changes to services, traffic patterns, or risk controls.

IV. KNOW YOUR CUSTOMER PROCEDURES

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 its voice service subscribers, whether a residential or business/commercial subscriber. 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 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 subscribers occur 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.

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

- 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 the Provider 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 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 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.

V. 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.

Further, for: (1) single line voice service subscribers the switching equipment has been set up to only accept calls from the number assigned to that subscriber; and (2) subscribers with multi-line telephone systems, the Provider screens all originating calls and only allows calls to be connected if the originating number matches one of the numbers assigned to the subscriber. These screening capabilities enable an automated and secure method of validating originating telephone numbers.

VI. 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 fully vetting such customers and performing telephone number validation on all international originated calls.

VII. KNOW YOUR UPSTREAM PROVIDER PROCEDURES

As a small provider of voice services, we use a very limited number of upstream providers. The Provider has longstanding relationships with these 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 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. Included as part of **Appendix A** to this Robocall Mitigation Plan document is a list of the Provider's current, immediate "Upstream Provider(s)" along with contact information for each.

VIII. ONGOING ROBOCALL MITIGATION PRACTICES

The Provider 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 the Provider 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:

1. initiating a traceback investigation.
2. verifying that the originating customer owns or is authorized to use the Caller ID number.
3. determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name.
4. terminating the party's ability to originate, terminate, or route calls on the Provider's network.
5. providing notice to law enforcement authorities.

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 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.
5. calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator.

IX. THIRD-PARTY ANALYTICS

The Provider relies on upstream carrier controls and internal monitoring rather than standalone third-party analytics platforms. As part of its architecture, the Provider restricts customer-site voice traffic to Bandwidth-approved IP address ranges and authorized Provider IPs, blocking all other voice traffic at the firewall.

Appendix A

Traceback Request Single Point of Contact:

Name: Sven Vazquez

Title: Systems/VOIP Engineer

Phone Number: 407.228.7290

Email Address: totalvoice@orlantech.com

Upstream Provider Information:

Name of Upstream Provider: Bandwidth.com

Nature of Business: Full-service SIP Provider with fraud analytics

Network Location of Upstream Provider: USA

Phone Number: 855-864-7776