

TechCore Concepts, LLC

Robocall Mitigation Plan

This Robocall Mitigation Plan is submitted by TechCore Concepts, LLC 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 that may use its service to originate calls.

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 has implemented the STIR/SHAKEN authentication framework through its upstream provider, Vitelity. As part of STIR/SHAKEN compliance, Vitelity will sign and provide attestation for outbound call services. No changes are required by Vitelity customers (Provider) as this is an inter-carrier connection. Additionally, signing will use a Vitelity certificate with unique customer identification so any complaints submitted through the robocall mitigation process via industry channels, can be traced to specific customers on the Vitelity platform.

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 **Worksheet A** to this plan, the Provider identifies a single point of contact for receiving all traceback requests.

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 voice service subscribers (business/commercial contracted customers). 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 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:

- 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 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 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.

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, both services connected via TDM or IP, 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, for both services connected via TDM or IP, 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.

INTERNATIONAL CALL ORIGINATORS

The Provider is not currently an international voice services provider and does not sell any services internationally.

KNOW YOUR UPSTREAM PROVIDER PROCEDURES

As a reseller of voice services, the number of upstream providers used by the Provider to receive and deliver its originated voice calls for termination are somewhat limited. The Provider has a longstanding relationship 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 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 **Worksheet 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.

ONGOING ROBOCALL MITIGATION PRACTICES

The Provider monitors the usage of its network and examines call detail records (CDRs) on a monthly basis for the purpose of detecting suspicious call activity and/or calling patterns and to determine customer usage. 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: 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 the Provider's network; and 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) use of IP restrictions for connectivity; (5) use of automated blacklisting; (6) use of additional software firewalls.

THIRD-PARTY ANALYTICS

The Provider also uses third-party call analytics to further assist and prevent the origination of illegal robocalls on its network. Included in **Worksheet A** is the name of the vendor(s) used along with a description of the call analytics system(s) used to identify and block illegal robocall traffic.

Worksheet A

TRACEBACK REQUEST SINGLE POINT OF CONTACT

Name: Andrew Amos

Title: CTO

Phone Number: 702.850.7272

Email Address: vendors@techcoreconcepts.com

UPSTREAM PROVIDER INFORMATION

Name of Upstream Provider: Sinch Voice\Intelliquest\Vitelity

Nature of Business: VoIP/SIP, vFax and SMS provider

Network Location of Upstream Provider: 317 Inverness Way South Ste 140
Englewood, CO 80112

Phone Number: (888) 898-4835

Fax Number: (303) 991-7999

Email Address: support@vitelity.net

CALL ANALYTICS VENDOR NAME AND DESCRIPTION OF SYSTEM

Name of Vendor: Sinch Voice\Intelliquest\Vitelity

Description of the call analytics system: TechCore Concepts, LLC utilizes a third-party “Analytics” platform provided by Sinch Voice to support the effectiveness of its Robocall Mitigation Plan. This includes, as examples, the use of “Telecom Fraud Prevention” and “Robocall and Telephone Denial of Service (TDos) Prevention” services, which include more specifically the use of the following methods/tools as a means of preventing and blocking fraudulent and illegal robocalls on its network: the use of CDRs and related reports for determining mitigation actions; use of SIP Analytics enabling real time traffic analysis and detection and mitigation of robocalls at origination; use of blacklisting and whitelisting to mitigate calls with specific attributes; use of CAPTCHA gateway services to distinguish whether calls are from humans or autodialers; use of a “Shield” database that screens calls at origination for calling numbers that are invalid, high-risk, or appear on “Do Not Originate” lists; and use of reputation look up services on calling numbers at origination.