

Robocall Mitigation Plan

Business Information

Verve Cloud, Inc
8023 Vantage Dr.
Suite 660
San Antonio TX 78230

Contact Information

George Robyn
VP of Engineering and DevOps
858-771-9815
grobyn@vervecloud.com

Overview

The Federal Communications Commission (“FCC” or “Commission”) requires all voice service providers (“VSPs”) to file robocall mitigation plans (“RMPs”) that, among other things, outline “reasonable steps” taken to avoid originating illegal robocalls.¹

In addition to the “reasonable steps,” the FCC requires that a RMP include:

- “know your customer” procedures;
- “know your upstream provider”;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Purpose

Verve is a small VSP dedicated to stopping illegal calls from traversing our network and monitoring the calls coming into our network. As certified in the FCC’s Robocall Mitigation Database, Verve has fully implemented STIR/SHAKEN. In compliance with the R&O, Verve submits this RMP and certification.

Know Your Customer (“KYC”)

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with Verve in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

¹ See *In the Matter of Call Authentication Trust Anchor; Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 2023) (“R&O”).

Verve's policy is that customers can only use a Caller ID if they own the number and it is hosted by one of Verve's voice carriers.

Verve's KYC program involves obtaining specific subscriber information when payment is made for services. This process includes collecting such information such as:

- physical business location;
- contact person(s); and
- nature of the customer's business.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59* (Rel. May 19, 2023) ¶¶ 49-51, Verve provides the following information concerning its upstream voice service carriers.

Verve has four upstream providers from which it receives voice traffic: Bandwidth, thinQ Technologies, Inc., Inteliquent, Inc. OBA Onvoy, Sinch ("Vitelity"), and Peerless Network, Inc. Verve collects information about these providers, including their physical business locations and contact persons. Additionally, Verve has master service agreements with these upstream providers and has received assurances in writing from their officials that they (i) sign calls transmitted to Verve, and (ii) will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Verve. Verve and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

Verve maintains an AUP that subscribers must sign before being permitted to use Verve's network. Among other things, the AUP prohibits:

- using the Services (as defined in the AUP) to transmit unsolicited e-mail messages, including, without limitation, unsolicited bulk email, where such emails could reasonably be expected to provoke complaints ("spam");
- using the service of another provider to send spam to promote a site hosted on or connected to the Verve Network;
- using the Services in order to (a) send e-mail messages which are excessive and/or intended to harass or annoy others, (b) continue to send e-mail messages to a recipient that has indicated that he/she does not wish to receive them, (c) send e-mail with forged TCP/IP packet header information, (d) send malicious e-mail, including, without limitation, "mailbombing", (e) send or receive e-mail messages in a manner that violates the use policies of any other Internet service provider, or (f) use an e-mail box exclusively as a storage space for data;
- using the Service to transmit excessive volumes of unsolicited commercial email messages or deliberately send excessively large attachments to one recipient;
- sending email messages or transmit any electronic communications using a name or address of someone other than the User for purposes of deception; and

- using the Service for transmission, distribution, retrieval, or storage of any information, data, or other material in violation of any applicable law or regulation.

Verve's contractual terms with subscribers specify that Verve may take action up to and including suspension or termination of service for violation of the AUP.

Mitigation During Service

Verve works with its upstream providers to (i) ensure that all subscribers can report any suspicious call connected through their account and (ii) to implement measures to ensure that future calls to/from a number associated with a suspicious can be blacklisted following a subscriber's report..

Analytics for Monitoring Traffic

Verve works with its upstream providers to monitor and identify behaviors which may indicate illegal call activity. Examples of calling patterns monitored are:

- anomalies in cost generated by calls from a single customer;
- multiple overlapping calls on the same account is a risk of not having a single subscriber using the service;
- velocity on initiate calls (synchron intervals, quick dialing back-to-back calls);
- recent volumes (last 60 min) vs weekly trends;
- number of unique destination numbers in a time frame (total account level);
- number of unique source numbers in a time frame (total and account level);
- and
- anomalies in call duration distribution (most calls having similar duration is not representative for residential service usage).

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Verve works with its upstream provider to follow defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and/or
- contacting the subscriber to understand his particular use case and validate that the activity belongs to that subscriber.

Verve uses the services of Transnexus (ClearIP) for call analytics.

Traceback

Verve follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations Verve commits to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Verve works with its upstream providers to investigate suspicious activity found by the carriers' monitoring systems or reported to Verve by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Verve contacting a subscriber to correct improper use of the applicable platform, or, if the subscriber does not respond or comply, to notify its upstream provider to block their use of the platform.

For all new and renegotiated Verve contracts governing the transport of voice calls, Verve will endeavor to contractually require Verve's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Verve's upstream providers have mechanisms to automatically block suspicious calls using internal analytics. If Verve and/or its upstream carriers identify suspected robocalling patterns that are confirmed with further investigation, Verve will take appropriate action which may include suspending or terminating the subscriber's use of Verve Verve's service.