

Robocall Mitigation Plan

Business Information

JV Connectivity

21218 St Andrews Blvd

#203

Boca Raton, FL 33433

JV Connectivity Contact
Information:

John Vance

Managing Director

(561) 827-5773

john@jvconnectivity.com

Overview

In the Commission's recent release, Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd. 2573 (2023) ("R&O"), it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "reasonable steps" taken to avoid originating illegal robocalls.

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

"know your customer" procedures;

"know your upstream provider";

ownership information;

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

JV Connectivity ("JV") is a small VSP dedicated to stopping illegal calls from traversing our network and monitoring the calls coming into our network. JV Connectivity is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, JV Connectivity was previously exempt from the FCC's STIR/SHAKEN rules. The R&O requires that pure resellers such as JV Connectivity now file RMPs. This document delineates JV Connectivity's RMP. Because JV Connectivity does not have access to the necessary infrastructure, it relies on its upstream carriers to assist in robocall mitigation. As delineated herein, JV Connectivity works closely with its upstream providers to carry out the required mitigation functions.

Know Your Customer ("KYC")

JV Connectivity maintains and implements KYC procedures as part of its robocall mitigation program, designed to reasonably verify the identity and legitimacy of its customers before enabling voice 2 3

1) AT&T

601 New Jersey Ave., NW
Suite 650
Washington DC 20001
Adam Panagia
g03115@att.com

JV Connectivity has master service agreements with its upstream providers and has received assurances from their officials that they have, and will continue to, sign calls transmitted to JV Connectivity and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to JV Connectivity. JV Connectivity 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")

JV Connectivity maintains an AUP that subscribers must sign before being permitted to JV Connectivity's network. Among other things, the AUP prohibits using its Services or related Software to upload, post, email, distribute, transmit, link, solicit or otherwise make available any Content or use our Services in any manner that:

1. is deceptive in a manner that is criminal or that is otherwise objectionable to us in our sole discretion, such as an offer to sell fraudulent goods or an impersonation of any person or entity or a misrepresentation of an affiliation with a person or entity;
2. specifically advertises firearms or ammunition, tobacco, alcohol, illegal drugs, or other contraband; and
3. constitutes unsolicited or unauthorized advertising, junk or bulk e-mail (SPAM), chain letters, or any other unsolicited commercial or non-commercial communication.

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

Mitigation During Service

JV Connectivity works with its upstream providers to ensure that all subscribers can report any suspicious call connected through their account and measures are set to prevent future calls from/to that individual numbers for all subscribers (none routed by the platform from that moment on - blacklisting). 4

Analytics for Monitoring Traffic

JV Connectivity works with its upstream providers to identify behaviors which indicate illegal call activity. Examples of calling patterns monitored:

- . anomalies in cost generated by calls from a single customer;
- . recent volumes (last 60 min) vs weekly trends; 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, JV Connectivity works with its upstream providers 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; and
- . contacting the subscriber to understand his particular use case and validate that the activity belongs to that subscriber.

No third-party vendors are involved in JV Connectivity's traffic analytics.

JV Connectivity follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, JV Connectivity will devote sufficient resources to provide prompt and complete resources to traceback requests. JV Connectivity commits to respond within 24 hours to all traceback requests from the FCC, 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.

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

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

Blocking

JV Connectivity will implement Do Not Originate requests it receives from ITG. JV Connectivity's upstream providers have mechanisms to automatically block suspicious calls using internal analytics. If JV Connectivity and/or its upstream carriers identify suspected robocalling patterns that are confirmed with further investigation, JV Connectivity will take appropriate action which may include suspending or terminating the subscriber's use of JV Connectivity's service. JV Connectivity will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including the state attorney general's office), as well as the FCC, and/or ITG; as well as documenting requests & actions taken in response thereto. 5

Plan Updates

This plan, along with industry best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. JV Connectivity will monitor industry best practices and continuously improve our internal processes to ensure this plan, and our system adapts to this ever-changing issue.

In the event of any material change to this plan, JV Connectivity will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update. 6

Certification of Leonid Levit

I, John Vance, CEO of JV Connectivity Inc. ("JV Connectivity"), do hereby certify, under penalty of perjury, the following:

(1) JV Connectivity, by virtue of its status as a "pure reseller" does not have access to the necessary infrastructure to implement STIR/SHAKEN, and therefore has not implemented STIR/SHAKEN in the IP portions of its network.

(2) JV Connectivity's Business name and primary address are as follows:

JV Connectivity
21218 St. Andrews Blvd
#203
Boca Raton, FL 33433

(3) JV Connectivity uses the following business names: JV Connectivity

(4) JV Connectivity has not previously used any other business name.

(5) The following individuals exercise management and control over JV Connectivity: John Vance

(6) JV Connectivity has no subsidiaries or affiliates.

(7) None of the persons/entities in items 5 – 6 above have had their licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.

(8) The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.

(9) JV Connectivity's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.

(10) JV Connectivity has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.

(11) JV Connectivity is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

(12) JV Connectivity is not required to have, and does not have an operating company number.

_____ X