

Robocall Mitigation Plan

Business Information

BVM Communication LLC
15 Woodland Avenue
Middlesex, NJ 08846

Contact Information

Bijal Patel
Member
(732) 668-5651
support@nexiptel.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

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

Our company takes several steps to avoid originating illegal robocalls. Given that our customers are primarily pharmacies and doctors' offices, we prioritize ensuring that all calls are legitimate and not disrupted by illegal robocalls. Additionally, we monitor the Call Detail Records (CDR) for any suspicious activity. We educate our customers about robocalls and encourage them to report any unusual activity to help maintain compliance with FCC regulations.

Know Your Customer ("KYC")

We provide services to health care providers (pharmacy, doctors' offices) and retail businesses like restaurants and UPS Stores. We manage the Caller ID on our PBX platform to make sure we provide correct caller ID for customers.

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 BVM in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

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

- federal tax ID;
- physical business location;
- contact person(s);
- 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, and 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, 38 FCC Rcd 5404 (2023), BVM provides the following information concerning its upstream voice service carrier.

BVM has five upstream providers from which it receives voice traffic:

1. Bandwidth Inc
900 Main Campus Drive
Suite 100
Raleigh NC 27606
Stephen Thayer
Email: voicesecurity@bandwidth.com
2. Inteliquent, Inc. DBA Onvoy, Sinch
550 W. Adams St.
Suite 900
Chicago IL 60661
Stacy Graham
Director, Assurance & Trust Services
Email: stacy.graham@sinch.com
Tel.: (217) 862-1953
3. Twilio Inc
101 Spear Street, 1st Floor
San Francisco CA 94105
Amy Holcroft
Tel: (415) 295-4909
Email: aholcroft@twilio.com

4. Intelepeer Networks LLC
18 Shrewsbury Drive
Rumson NJ 07760
Frank Lauria
Tel.: (732) 713-3562
Email: frank.lauria@esplicity.com
5. HFA Services LLC d/b/a Skyetel
2901 Clint Moor Road
Suite 2, #215
Boca Raton FL 33496
Joey Buchbinder
Tel.: (561) 282-5500
Email: jbuchbinder@skyetel.com

BVM 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 BVM and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to BVM. BVM 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")

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

- using the system for originating robocalls, illegal telemarketing, or spam;
- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- sending unsolicited bulk communications (email, voice, or otherwise);
- violating any applicable law (including any activity that violates local, state, federal, or international law, such as fraud, phishing, or any form of unauthorized access); and
- interfering with the operation of the network, including but not limited to excessive call traffic or service disruptions.

Under BVM's AUP, subscribers must comply with all applicable laws, regulations, and policies regarding the use of BVM's network and services. Moreover, subscribers are responsible for ensuring that their use of the services does not disrupt or harm the network, including preventing fraudulent activities or illegal calls. Subscribers are encouraged to report any suspicious activity or violations of this policy.

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

Telephone Number Authorization

New subscribers placing outbound calls can only use Caller IDs which have been purchased through our platform or ones verified through automated-number-validation voice call. Subscribers can sign a form allowing them to use Caller IDs not purchased through our platform or verified by validation call

for outbound calls, functionality that is restricted to customers with whom we've had human contact by phone call or in-person. This form:

- prohibits the sending of outbound traffic via the PSTN with Caller IDs not owned by the customer or the customer's subscribers; and
- states that, if NKVoice receives notice that the Customer's outbound calls through our platform are deemed to be spam, NKVoice has the right to disconnect the service immediately and without notice.

Analytics for Monitoring Traffic

BVM works with its upstream provider to identify behaviors which indicate illegal call activity. Examples of calling patterns monitored:

- 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, BVM 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, such as a high call volume;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his particular use case and validate that the activity belongs to that subscriber.

Because BVM does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in BVM's analytics.

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

BVM works with its upstream provider to investigate suspicious activity found by the carrier's monitoring systems or reported to BVM by subscribers or third parties. The investigation could potentially result in opening a traceback request or with BVM 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 BVM contracts governing the transport of voice calls, BVM will endeavor to contractually require BVM's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

BVM Communication LLC follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, BVM will devote sufficient resources to provide prompt and complete resources to traceback requests. NKVoice commits to responding to traceback requests fully within 24 hours.

Blocking

Our company promptly responds to Do Not Originate (DNO) requests from the Industry Traceback Group (ITG). We validate the request, block unauthorized use of the specified numbers, and notify affected customers if applicable. Actions are documented, and we cooperate fully with the ITG and regulatory authorities to prevent further abuse.

BVM will implement Do Not Originate requests it receives from ITG. BVM's upstream provider has mechanisms to automatically block suspicious calls using internal analytics. If BVM and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, BVM will take appropriate action which may include suspending or terminating the subscriber's use of BVM BVM's service. BVM 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.

Plan Updates

This plan, along with industry best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. BVM 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, BVM 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.

Certification of Bijal Patel

I, Bijal Patel, Owner of BVM, do hereby certify, under penalty of perjury, the following:

- (1) BVM Communication LLC ("BVM"), 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) BVM 's Business name and primary address are as follows:

BVM Communication LLC
15 Woodland Avenue
Middlesex, NJ 08846
- (3) BVM uses the following d/b/a name: NexIPTeL.
- (4) BVM has not previously used any other business names.
- (5) The following persons own more than 10% of BVM each: Bijal Patel and Bilva Patel.
- (6) The following persons exercise management and control over BVM: Bijal Patel and Bilva Patel.
- (7) BVM has no subsidiaries or affiliates.
- (8) 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.
- (9) 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.
- (10) BVM's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (11) BVM has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (12) BVM is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (13) BVM is not required to have, and does not have an operating company number.

Bijal Patel

Date: _____