

Robocall Mitigation Plan

Business Information

FAVE3 LLC d/b/a Vela Mobile
1371 San Remo Lane
League City, TX
77573

Contact Information

David D. Selmon Jr.
Chief Strategy Officer
8326540703
davidselmon@vela-mobile.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 an 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

FAVE3 LLC d/b/a Vela Mobile ("Vela Mobile") is a small VSP dedicated to stopping illegal calls from traversing our network and monitoring the calls coming into our network. Vela Mobile is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, Vela Mobile was previously exempt from the FCC's STIR/SHAKEN rules. The R&O requires that pure resellers such as Vela Mobile now file RMPs. This document delineates Vela Mobile's RMP. Because Vela Mobile does not have access to the necessary infrastructure, it relies on its upstream carrier to assist in robocall mitigation. As delineated herein, Vela Mobile works closely with its upstream provider to carry out the required mitigation functions.

Vela Mobile monitors customer activity, maintains customer verification procedures, investigates suspicious traffic patterns, cooperates with traceback requests, and relies upon upstream carriers' STIR/SHAKEN implementation and call analytics systems to identify and mitigate unlawful robocall traffic.

Know Your Customer ("KYC")

Vela Mobile requires customers to provide identifying information during activation, including name, address, telephone number, email address, and payment information. The Company monitors account activity, investigates suspicious usage patterns, restricts fraudulent activity, and reserves the right to suspend or terminate service for violations of its Acceptable Use Policy.

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), Vela Mobile provides the following information concerning its upstream voice service carrier.

Vela Mobile receives voice traffic from one upstream provider which whom it has a master service agreement. The upstream provider has assured Vela Mobile that it has, and will continue to, sign calls transmitted to Vela Mobile and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Vela Mobile. Vela Mobile and its upstream provider have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

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

- Illegal robocalling,
- Caller ID spoofing,
- Fraudulent telecommunications activity,
- Transmission of unlawful traffic, and
- Violation of federal or state telecommunications laws

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

Mitigation During Service

Vela Mobile works with its upstream provider 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). These features are:

- VoIP-originated calls are signed with subscriber caller ID only after number validation via SMS; and
- requiring authentication to initiate any call, or a whitelist of originating numbers that is under customer's control.

Analytics for Monitoring Traffic

Vela Mobile works with its upstream telecommunications providers and fraud management partners to identify calling behaviors that may indicate fraud, abuse, or other unauthorized use of its service.

As a non-facilities-based telecommunications provider, many of these monitoring capabilities are performed by Vela Mobile's upstream providers using network and traffic analytics.

Examples of calling patterns that may be monitored include:

- Unusual or excessive charges generated by calls from a single subscriber or account;
- Multiple simultaneous or overlapping calls from the same account, which may indicate unauthorized account sharing, SIM misuse, or other fraudulent activity;
- High call initiation velocity, including rapid sequential dialing, synchronized call attempts, or repeated back-to-back outbound calls;
- Significant increases in recent call volume (for example, activity during the previous 60 minutes compared to historical usage patterns);
- An unusually high number of unique destination telephone numbers contacted within a defined period;
- An unusually high number of unique originating telephone numbers associated with an account within a defined period; and
- Unusual call duration patterns, such as a high concentration of calls with nearly identical durations, which may indicate automated calling, traffic pumping, or other non-standard usage patterns.

These monitoring activities are intended to protect Vela Mobile, its customers, and its network partners from fraud, abuse, and unlawful use of telecommunications services. Detection of one or more of these indicators does not, by itself, establish fraudulent or unlawful activity but may result in further review or investigation in accordance with Vela Mobile's policies and applicable law.

Investigate Suspicious Activity

Vela Mobile reviews customer complaints, investigates suspicious traffic patterns, cooperates with other stakeholders regarding traceback requests, coordinates with its upstream provider, and suspends or terminates accounts engaged in unlawful activity.

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

Investigation procedures may include, but are not limited to:

- Reviewing recent and historical call detail records ("CDRs") and comparing activity against expected usage patterns;
- Reviewing recent account activity, purchases, activations, and account changes;
- Determining whether a network, provisioning, or system issue may have contributed to the observed activity;
- Verifying that the originating call path and network routing are valid;
- Contacting the subscriber, when appropriate, to confirm the legitimacy of the observed calling activity and better understand the subscriber's intended use of the Service; and
- Coordinating with upstream telecommunications providers, as appropriate, to investigate suspected fraudulent or unlawful traffic.

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

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

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

Blocking

Vela Mobile will implement Do Not Originate requests it receives from ITG. Vela Mobile's upstream provider has mechanisms to automatically block suspicious calls using internal analytics. If Vela Mobile and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, Vela Mobile will take appropriate action which may include suspending or terminating the subscriber's use of Vela Mobile Vela Mobile's service. Vela Mobile 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. Vela Mobile 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, Vela Mobile will file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of David D. Selmon Jr.

I, David D. Selmon Jr., Chief Strategy Officer of FAVE3 LLC d/b/a Vela Mobile ("Vela Mobile"), do hereby certify, under penalty of perjury, the following:

- (1) Vela Mobile, 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) Vela Mobile 's Business name and primary address are as follows:

FAVE3 LLC d/b/a Vela Mobile
1371 San Remo Lane
League City, TX
77573
- (3) FAVE3 LLC uses the doing-business-as name of "Vela Mobile" and has no other business names in use.
- (4) Vela Mobile has not previously used any other business name.
- (5) Vela Mobile has the following principals: Harold Perez, David D. Selmon Jr., David Selmon Sr., Bernadette Selmon.
- (6) Vela Mobile has the following parent companies: Vale Holdings LLC and D & B Ventures LLC.
- (7) Vela Mobile 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) Vela Mobile's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (11) Vela Mobile has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (12) Vela Mobile is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (13) Vela Mobile is not required to have and does not have an operating company number.



David D. Selmon Jr.