

Robocall Mitigation Plan

Business Information

Moola Cloud, LLC d/b/a Black Wireless
1120 Ave of the Americas
4th Floor
New York, NY, 10036

Contact Information

Anthony Cancelleri
VP of Operations
239-631-0544 / 855-511-3390
Tony@black011.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

Moola Cloud, LLC d/b/a Black Wireless ("Black Wireless") is a small VSP dedicated to stopping illegal calls from traversing our network and monitoring the calls coming into our network. Black Wireless is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, Black Wireless was previously exempt from the FCC's STIR/SHAKEN rules. Black Wireless is a reseller of voice services to retailers and/or end users and does not support transit, wholesale VoIP termination, or enterprise dialer traffic on its wireless platform.

The R&O requires that pure resellers such as Black Wireless now file RMPs. This document delineates Black Wireless's RMP. Because Black Wireless does not have access to the necessary infrastructure, it relies on its upstream carrier to assist in robocall mitigation. As delineated

herein, Black Wireless works closely with its upstream provider to carry out the required mitigation functions.

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 Black Wireless in which we transmit, originate, and/or terminate calls based on behalf of the subscriber. Accounts are strictly tied to specific SIM profiles.

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

- physical business location;
- credit card number;
- 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), Black Wireless provides the following information concerning its upstream voice service carrier.

Black Wireless has one upstream provider from which it receives voice traffic:

Airespring, Inc.
600 Cleveland Street
Suite 226
Clearwater FL 33755
David Hess
david.hess@airespring.com

Black Wireless has a master service agreement with its upstream provider and has received assurances from its officials that it has, and will continue to, sign calls transmitted to Black Wireless and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Black Wireless. Black Wireless 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")

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

- unsolicited or unauthorized advertising, junk or bulk e-mail (SPAM), chain letters, or any other unsolicited commercial or non-commercial communication;
- deceptive conduct; and
- creating a false identity for the purpose of misleading others; and
- using Black Wireless's service to engage in or in connection with fraudulent activities.

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

Mitigation During Service

Black Wireless 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 those 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

Black Wireless works with its upstream provider to identify behaviors which indicate illegal call activity. Black Wireless relies on its upstream provider's infrastructure to monitor all traffic profiles for HVSD (high volume, short duration) call patterns and utilizes its own SIM management platform-level data alongside upstream carrier analytics to flag automated dialer behavior and strictly enforces non-commercial retail usage thresholds on all consumer accounts to block automated spam generation.

Examples of calling patterns monitored include:

- 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, Black Wireless works with its upstream provider to follow defined procedures on investigating such subscribers.

Upon system alerts or third-party complaints, the compliance team performs an immediate CDR (Call Detail Record) audit of the flag. If an account exhibit robocall metrics (e.g., hundreds of

calls per minute with a low completion rate), the account is immediately suspended pending investigation.

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
- contacting the subscriber to understand his particular use case and validate that the activity belongs to that subscriber.

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

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

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

Blocking

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

Certification of Anthony Cancelleri

I, Anthony Cancelleri, VP of Operations of Moola Cloud, LLC d/b/a Black Wireless ("Black Wireless"), do hereby certify, under penalty of perjury, the following:

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

Moola Cloud, LLC d/b/a Black Wireless
1120 Ave of the Americas
4th Floor
New York, NY, 10036
- (3) Moola Cloud, LLC uses the business names "Black Wireless" and "Black 011."
- (4) Black Wireless has not previously used any other business name.
- (5) Black Wireless has the following parent companies and principals: The OLB Group, Inc., Anthony Cancelleri, Ronny Yakov. Neither of these persons/entities has had their licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding. Black Wireless does not have any affiliates.
- (6) 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.
- (7) Black Wireless's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (8) Black Wireless has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (9) Black Wireless is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (10) Black Wireless is not required to have and does not have an operating company number.



Anthony Cancelleri

08/08/2026