

Robocall Mitigation Plan

Business Information

HeadsUp Holdings, Inc., d/b/a Cloaked, Inc.
1075 Westford Street
Suite 305
Lowell, MA 01851-2845

Contact Information

Arjun Bhatnagar
CEO
617.468.5214
arjun@cloaked.id

Overview

In the Commission's release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (released March 17, 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

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

Know Your Customer

The identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber.

New Subscribers

New Subscribers provide, as needed based on the product or service entered into, their name, email address, credit card information [via Stripe], and contact phone number to Cloaked. If necessary, Cloaked is able to communicate with an underlying network to identify a customer.

Acceptable Use Policy

Cloaked maintains an Acceptable Use Policy ("AUP") that subscribers must agree to before being permitted to use Cloaked's network. Among other things, the AUP prohibits:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- violating any applicable local, state, or federal law;
- violating applicable industry accepted guidelines; and
- using Cloaked's service to engage in or in connection with fraudulent activities.

Cloaked's AUP specifies that Cloaked may take action, including suspension or termination of service, for violation of same.

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, Cloaked provides the following information concerning its upstream voice service carrier. Cloaked's upstream provider is:

Bandwidth, Inc.
2230 Bandmate Way
Raleigh, NC 27607
Stephen Thayer
voicesecurity@bandwidth.com

Cloaked and its upstream provider have no contractual provisions regarding robocall mitigation. But, Cloaked and its upstream provider work together to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests. Cloaked's upstream provider is listed as STIR/SHAKEN compliant in the Robocall Mitigation Database.

Telephone Number Authorization

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify an outbound caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by Cloaked and/or obtained by Cloaked from one of Cloaked's underlying carriers for use by the subscriber. In most cases, Cloaked directly manages the TNs used by its subscribers. Cloaked tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Cloaked's assignment of the TN to its subscriber.

Mitigation During Service

Cloaked 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

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

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

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

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

Blocking

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

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. Cloaked will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

In the event of any material change to this plan, Cloaked 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 Arjun Bhatnagar

I, Arjun Bhatnagar, CEO of Cloaked, Inc HeadsUp Holdings, Inc., d/b/a Cloaked, Inc. ("Cloaked"), do hereby certify, under penalty of perjury, the following:

- a. Cloaked, 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
- b. STIR/SHAKEN in the IP portions of its network.
- c. Cloaked's Business name and primary address are as follows:

HeadsUp Holdings, Inc., d/b/a Cloaked, Inc.
1075 Westford Street
Suite 305
Lowell, MA 01851-2845

- d. Except for Head's Up Holdings, Inc. Cloaked has no other business names in use.
- e. Cloaked has not previously used any other business name.
- f. 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.
- g. Cloaked's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- h. The entities with 10% or more ownership interest in Cloaked are Arjun Bhatnagar and Abhijay Bhatnagar.
- i. Cloaked has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- j. Cloaked is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- k. Cloaked is not required to, and does not have, an operator company number.


Arjun Bhatnagar