

Robocall Mitigation Plan

Business Information

RedChirp LLC
6501 E. Greenway Parkway
Suite 103-168
Scottsdale AZ 85254

Contact Information

James Harry Kane, Jr.
CEO
315-212-3517
jim.kane@redchirp.com

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 (rel. 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

RedChirp LLC ("RedChirp") is a small VSP dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network. RedChirp is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, RedChirp was previously exempt from the FCC's STIR/SHAKEN rules. The R&O requires that pure resellers such as RedChirp now file RMPs. This document delineates RedChirp's RMP. Because RedChirp does not have access to the necessary infrastructure, it relies on its upstream carrier to assist in robocall mitigation. As delineated herein, RedChirp 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 RedChirp in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

RedChirp requires new subscribers to provide full corporate contact information, including mailing address, responsible employee name, and tax identification (EIN) number to sign up for service. RedChirp does not offer service to any organization that cannot pass secondary vetting by The Campaign Registry (EIN, corporate name must match databases, etc.). Caller ID information must match the corporate contact information provided.

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, RedChirp provides the following information concerning its upstream voice service carrier

Bandwidth.com
900 Main Campus Dr
Suite 500
Raleigh NC 27606
John Anthony
jwanthony@bandwidth.com

To the extent that RedChirp were to receive information from law enforcement or other sources that a customer is engaged in illegal robocalling, our policy is to cooperate fully, including providing the identity of any suspected illegal robocaller, pursuant to legal service or process. While RedChirp's agreement with its upstream provider contains no provisions specific to robocall mitigation, RedChirp has received assurances from that provider that it has, and will continue to, sign calls transmitted to RedChirp, and will abide by the FCC's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic.

Acceptable Use Policy ("AUP")

RedChirp maintains an AUP that subscribers must agree to before being permitted to use RedChirp's system. RedChirp's AUP is here: <https://files.redchirp.com/terms-of-use.pdf>.

Analytics for Monitoring Traffic

RedChirp works with its upstream provider to identify behaviors which indicate illegal call activity. Subscribers must specifically request the ability to place outbound calls and supply their use case before outbound dialing is enabled. Subscribers have very low outbound call quotas (typical limits are 50 calls per day or less) and must apply for any increase in this limit. RedChirp reviews outbound call logs and analytics regularly to monitor for any possible abuse.

No third parties are involved in deploying RedChirp's analytics.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, RedChirp works with its upstream provider to follow defined procedures on investigating such subscribers. RedChirp actively monitor calls from all customers and have quotas in place per customer that limit their outbound calling to a small number of calls per day. The outbound call logs are checked manually, and the customers are blocked if necessary.

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

Blocking

RedChirp will implement Do Not Originate requests it receives from the ITG. RedChirp's upstream provider has mechanisms to automatically block suspicious calls using internal analytics. If RedChirp and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, RedChirp will take appropriate action which may include suspending or terminating the subscriber's use of RedChirp's service. RedChirp will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement, the FCC, and 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. RedChirp 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, RedChirp 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 James Harry Kane, Jr.

I, James Harry Kane, Jr., CEO of RedChirp LLC ("RedChirp"), do hereby certify, under penalty of perjury, the following:

- a. RedChirp, 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.
- b. RedChirp's business name and primary address are as follows:

RedChirp LLC
6501 E. Greenway Parkway
Suite 103-168
Scottsdale AZ 85254

- c. RedChirp has no other business names in use.
- d. RedChirp has not previously used any other business name.
- e. 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.
- f. RedChirp's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- g. The persons that have 10% or more ownership interest in RedChirp are: James Harry Kane Jr., Jennie Kathleen Gilbert, and Scott Alexander Gilbert. RedChirp has no affiliates or subsidiaries.
- h. RedChirp has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- i. RedChirp is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- j. RedChirp is not required to, and does not have, an operating company number.


James Harry Kane, Jr.