

Robocall Mitigate Policy

Objective: Establish and follow a policy that is compliant with the FCC's "Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking , WC Docket No. 17-97"

Cirrus Networks, Inc. is a non-facilities-based reseller of voice services. We do not operate the network infrastructure necessary to implement STIR/SHAKEN and therefore do not have a STIR/SHAKEN implementation obligation. All calls originated by our customers are handed off directly to our upstream wholesale provider, which is fully responsible for STIR/SHAKEN call authentication.

Cirrus Networks, Inc. has implemented a robocall mitigation program appropriate for a reseller. We verify the identity of our customers, require valid use of telephone numbers, and monitor for fraudulent or suspicious traffic. Any unlawful or suspicious traffic is addressed promptly, including mitigation actions up to and including disconnection of the customer.

As a reseller, we do not claim "complete" or "partial" STIR/SHAKEN implementation. Our upstream provider(s) are responsible for authentication of calls using their SPC token and certificate.

Cirrus Networks, Inc. understands and is committed to implementing policies and procedures to ensure we are meeting our obligations towards eliminating illegal robocall activities in these three key areas - responding promptly to legal traceback requests, prevention of robocall origination from our platform, and mitigation of illegal calls should they occur.

This mitigation plan is submitted on behalf of Cirrus Networks, Inc.

Cirrus Networks, Inc. end user services are subject to restrictions contained in its legal notices and all executed services orders include the requirement that service is provided pursuant to its terms of service requirements.

Existing TOS prohibit activities normally associated with RoboCalling including, but not limited to:

- Using any autodialing services

- Providing altered or false information about the identity of the sender or the origin of a phone call
- Violating any applicable local, state, or federal law; using the Cirrus Networks, Inc. service to engage in fraudulent activities.

Cirrus Networks, Inc. end users are notified that Cirrus Networks, Inc. may take action up to suspension or termination of service for violation of the TOS.

Cirrus Networks, Inc. utilizes the mitigation technique of “Know Your Customer.” Cirrus Networks, Inc. provides voice service for mainly K-12 school systems or small to medium size businesses. Cirrus Networks, Inc. provides no residential service, currently.

Cirrus Networks, Inc. screens all new customers requesting service:

- Our customers are K-12 school systems or small to medium size businesses in our local service territory.
- We meet face to face with each customer to confirm the number of voice lines being requested
- We manage the phone system for all our voice service customers. This includes setting the caller ID for each extension. Limited access is provided to customers to reduce the chance of spoofing caller ID.
- We do not service large commercial customers or VoIP wholesale customers.

Cirrus Networks, Inc. requires all clients of our managed telephony services to provide detailed information about their organization and provide verified contact details in order to enter into an agreement for service. We have direct working relationships with all of our customers and are therefore aware of their requirements and intents for our services. By knowing our customer, we believe we can effectively monitor usage and flag unusual activity using our account monitoring tools. Additionally, as a provider exclusively of managed services, we maintain direct technical control of all equipment interconnected to our platform and can therefore prevent valid end users from utilizing any form of autodialing or mass calling technologies to affect illegal robocall activity and we control all mechanisms related to generating the CLID data associated with outbound calls.

Cirrus Networks, Inc. will actively cooperate with the traceback community including the FCC, law enforcement, and The Industry Traceback Group to investigate and stop illegal robocalls. Cirrus Networks, Inc. will dedicate sufficient resources to provide prompt and complete responses to traceback requests.