

Robocall Mitigation Plan

Business Information

Marlink, Inc. ("Marlink")
3327 South Sam Houston Parkway East
Suite 100
Houston, TX 77047

Contact Information

Pauline Rutenberg
General Counsel
+31 630 363 989
traceback@marlink.com

Overview

Pursuant to paragraphs 69-72 of the Federal Communications Commission's ("FCC," or "Commission") *Call Authentication Trust Anchor*, Sixth Report & Order and Further Notice of Proposed Rulemaking ("6th Report & Order") in WC Docket No. 17-97, FCC 23-18 (rel. March 17, 2023) and 47 C.F.R. § 64.6304(d), Marlink, which is a satellite telecommunications company and a domestic small voice provider, has an indefinite extension from the requirement to be STIR/SHAKEN compliant.

The 6th Report & Order also states 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;
- 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.

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 Marlink in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

From the technical side, we install the physical phones onboard the customers' vessels. We configure the phones with full E.164 numbers as caller ID, and we only allow calls from the caller IDs we have registered for our customers on our network.

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

- physical business location;

- 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, FCC 23-37_L (rel. May 19, 2023) ¶¶ 49-51, Marlink provides the following information concerning its upstream voice service carrier.

Marlink has two upstream providers from which it receives voice traffic directly:

Voxbone SA
900 Main Campus Drive
Suite 100
Raleigh NC 27606
Stephen Thayer
voicesecurity@bandwidth.com

Sinch Voice (dba Inteliquent, a Sinch company)
One North Wacker, Suite 2500
Chicago, IL, 60606
Gary Tabachnik
gary.tabachnik@sinch.com

Marlink has received assurances from its upstream providers' officials that it has, and will continue to, sign calls transmitted to Marlink and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Marlink. Marlink 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")

Marlink maintains an AUP that subscribers must agree to before being permitted to use Marlink'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 Marlink's service to engage in or in connection with fraudulent activities.

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

Analytics for Monitoring Traffic

Marlink works with its upstream providers 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, Marlink works with its upstream providers 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.

Numbers are assigned to SIP phones that are delivered behind Marlink satellite services. The phones are fully managed by Marlink, so the accounts can only be used via physical handsets. Due to the cost of the satellite service most customers make very few calls. Marlink has automated scripts in place that generate warnings if there is a suspicious number of calls from one customer.

We actively monitor calls from all customers, and have alarms triggered when there are large volumes of calls. The alarms are checked manually, and the customers are blocked if necessary.

No third-party vendors are involved in Marlink's analytics.

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

Marlink works with its upstream providers to investigate suspicious activity found by the carrier's monitoring systems or reported to Marlink by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Marlink 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 Marlink contracts governing the transport of voice calls, Marlink will endeavor to contractually require Marlink's subscribers to cooperate in traceback investigations by

identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Marlink will implement Do Not Originate requests it receives from the ITG. Marlink's upstream providers have mechanisms to automatically block suspicious calls using internal analytics. If Marlink and/or its upstream carrier identify suspected robocalling patterns that are confirmed with further investigation, Marlink will take appropriate action which may include suspending or terminating the subscriber's use of Marlink's service. Marlink 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. Marlink 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, Marlink 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 Pauline Ruitenberg

I, Pauline Ruitenberg, General Counsel of Marlink, do hereby certify, under penalty of perjury, the following:

(1) Marlink, as a satellite telecommunications company and a domestic small voice provider, is exempt from the requirement to implement STIR/SHAKEN, and therefore has not implemented STIR/SHAKEN in the IP portions of its network.

(2) Marlink 's Business name and primary address are as follows:

Marlink, Inc.
3327 South Sam Houston Parkway East
Suite 100
Houston, TX 77047

(3) Marlink has no other business names in use.

(4) Marlink has not previously used any other business name.

(5) The following persons/entities own more than 10% of Marlink: No natural person has a direct indirect ownership/controlling interest of 10% or more of Marlink.

The Marlink Group, which includes Marlink, Inc. and its Norwegian affiliate, Marlink AS, is for the majority owned by Providence Equity Partners ("Providence") and Seven2. Providence and Seven2 are regulated private equity investment advisers/fund managers subject to extensive (US and EU) anti-money laundering laws and regulations. Providence, together with its co- investor Ardian Holding, controls around 58% of Marlink, Seven2 around 36% and the remaining percentages of around 6% is held by other minority shareholders including senior management and employees of Marlink.

(6) The following person(s) are Marlink's principals:

- Alexandre De Luca: Director – Vice President
- Erik Ceuppens: Director – Chief Executive Officer
- Nathalie Senechault: Director – Chief Financial Officer and Treasurer
- Mike Neugebauer: Director (chairman) – President, Americas
- Tore Morten Olsen: Director – Vice President
- Pauline Ruitenberg – Secretary

(7) The following persons/entities are Marlink's subsidiaries/affiliates:

Marlink has approximately 50 subsidiaries/affiliates worldwide, including Marlink, Inc's. Norwegian affiliate, Marlink AS, with which it collaborates on provision of services to Earth Stations on Vessels.

(8) None of the persons/entities in items 5 – 7 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) Marlink's role in the call chain is that of a voice service provider without a STIR/SHAKEN

obligation.

- (11) Marlink has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (12) Marlink is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

/ Pauline Ruitenber
Pauline Ruitenber, General Counsel

Dated: February 20, 2026