

Robocall Mitigation Plan

Business Information

Coretek, LLC
34900 Grand River Avenue
Farmington Hills, MI 48335

Contact Information

Jonathan Koopman
Chief Financial Officer
Jonathan.koopman@coretek.com
+1248-741-1405

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 (adopted March 16, 2023) 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 includes:

- "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.

Purpose

Coretek, LLC is a small VSP dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network. Coretek is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. Because Coretek does not have access to the necessary infrastructure, it is not required to be STIR/SHAKEN compliant. Coretek works closely with its upstream providers 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 Coretek in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

Coretek KYC program obtaining specific information before allowing a potential subscriber to use our services. This process includes collecting business and contact details (company name, address, tax ID, authorized representative info), and requiring proof of identity and/or incorporation documents.

Moreover, Coretek accept payments only through approved billing methods (e.g., credit card, ACH, wire transfer). Coretek periodically reviews and updates customer records.

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, Coretek provides the following information concerning its upstream voice service carriers:

Altigen Communications, Inc.
39899 Balentine Drive
STE112
Newark, California, 94560

Coretek has received assurances from its upstream providers that they will continue to sign calls transmitted to Coretek and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Coretek. Coretek and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Telephone Number Analytics

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify the 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 Coretek and/or obtained by Coretek from Coretek's underlying carriers for use by the subscriber. In most cases, Coretek directly manages the TNs used by its subscribers. Coretek tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Coretek's assignment of the TN to its subscriber.

Analytics for Monitoring Traffic

Coretek works with its upstream carriers to analyze high-volume voice traffic in order to identify and monitor patterns consistent with robocalls. If Coretek detects a calling pattern consistent with illegal robocalls, we will identify the party and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our system.

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).

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

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Coretek works with its upstream providers to follow defined procedures on investigating such subscribers. These procedures include:

- 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.

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

Coretek works with its upstream providers to investigate suspicious activity found by the carriers' monitoring systems or reported to Coretek by subscribers or third parties. An investigation could potentially result in opening a traceback request or with Coretek 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(s) to block their use of the platform.

Coretek certifies that it will respond to all traceback requests within 24 hours of receiving same.

Blocking

Coretek will implement Do Not Originate requests it receives from the ITG. Coretek works with its upstream providers to automatically block suspicious calls using analytics. If those analytics reveal suspected robocalling patterns that are confirmed with further investigation, Coretek will take appropriate action which may include suspending or terminating the subscriber's use of Coretek's network and utilizing service restriction blocks. Coretek will cooperate with Investigative Bodies 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. Coretek will monitor industry best practices and continuously improve our internal processes to ensure this plan, and our system adapt to this ever-changing issue.

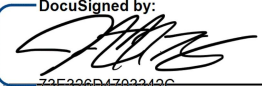
In the event of any material change to this plan, Coretek will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of Steve Thompson

I, Jonathan Koopman, Chief Financial Officer of Coretek, LLC, do hereby certify, under penalty of perjury, the following:

- (1) Coretek, 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) Coretek's business name and primary address are as follows:

Coretek, LLC
34900 Grand River Avenue
Farmington Hills, MI 48335
- (3) Coretek's dba is Coretek LLC
- (4) Coretek has not previously used any dba except Coretek, Coretek Services, Coretek Inc.
- (5) The following person owns more than 10% of Coretek: Ron Lisch 61%; Ray Jaksic 34%.
- (6) Coretek has no subsidiaries or affiliates.
- (7) Neither Coretek nor any of the persons listed herein have been subject to an FCC enforcement proceeding or have been forbidden to file in the Robocall Mitigation Database.
- (8) 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.
- (9) Coretek's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (10) Coretek does not have, and is not required to have, an operator company number.

DocuSigned by:

79E326B4703342C...
Jonathan Koopman

Chief Financial Officer, Coretek, LLC