

Robocall Mitigation Plan

Business Information

Advanced Technology Solutions, Inc. d/b/a K&S Computing
218 N Greenwood Ave
Fort Smith AR 72901

Contact Information

S. Mike Kimberling
President
(479) 459-4131
billing@kscomputing.biz

Overview

In the Commission's recent 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

Advanced Technology Solutions, Inc. d/b/a K&S Computing ("K&S") is dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. This document delineates K&S's RMP.

As certified in the FCC's Robocall Mitigation Database, K&S has fully implemented STIR/SHAKEN. In compliance with the R&O, K&S submits this RMP and certification.

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 K&S in which we transmit, originate, and/or terminate calls on behalf of the subscriber.

K&S's KYC program involves obtaining specific subscriber information. This process includes collecting such information such as:

- physical business location;

- contact person(s);
- email; and
- EIN.

We have existing relationships with all our customers beyond VoIP services. We have visited their physical premises and provide their IP support. Customers cannot purchase VoIP minutes, in house personnel manually funds their VoIP accounts. Customers have to provide a verified business name, address, phone number and banking info. Caller ID info (including the phone number listed for all outbound calls) is configured solely by in-house technical personnel.

We only provide hosted PBX to a handful of long-term IT customers. We control the PBX including all its configuration and only provide desk phones to end users. The PBXs are firewalled extensively, and call volume is closely monitored.

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, K&S provides the following information concerning its upstream voice service carrier.

K&S has one upstream provider from which it receives voice traffic:

VoIP Innovations, LLC
One Penn Center West
Suite 400
Pittsburgh PA 15276
Cameron Nutter
cnutter@sangoma.com

K&S has a master service agreement with its upstream provider and has received assurances in writing from its officials it has, and will continue to, sign calls transmitted to K&S, and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to K&S. K&S 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")

K&S maintains an AUP that subscribers must agree to before being permitted to use K&S'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 law;
- violating applicable industry standards;
- using K&S's service to engage in or in connection with fraudulent activities;
- calls that are unlawful, harassing, libelous, invasive of another's privacy, abusive, threatening, obscene or that infringes the rights or intellectual property of others.

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

Telephone Number Authorization

New subscribers placing outbound calls can only use Caller IDs which have been purchased through our platform or ones verified through automated-number-validation voice call. Subscribers can sign a form allowing them to use Caller IDs not purchased through our platform or verified by validation call for outbound calls, functionality that is restricted to customers with whom we've had human contact by phone call or in-person. This form:

- prohibits the sending of outbound traffic via the PSTN with Caller IDs not owned by the customer or the customer's subscribers; and
- states that, if K&S receives notice that the Customer's outbound calls through our platform are deemed to be spam, K&S has the right to disconnect the service immediately and without notice.

Analytics for Monitoring Traffic

K&S works to detect a calling pattern consistent with illegal robocalls. If such a call is detected, we will identify the party that is using our network to originate those calls 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 network.

K&S uses VoIP Innovations & CSF for traffic analytics.

Monitoring

K&S works with its underlying provider to detect a calling pattern consistent with illegal robocalls. If such a call is detected both parties will identify the party that is using K&S's network to originate those calls 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 network.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, our risk prevention team is alerted which follows the defined procedures on investigating such subscribers. For example, excessive call volume generates an alert that gets investigated by a specialist

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 or her particular use case and validate that the activity belongs to that subscriber.

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

Blocking

K&S will implement Do Not Originate requests it receives from the ITG. If K&S's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, K&S will take appropriate action which may include suspending or terminating the subscriber's use of teschmied's network. K&S will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including the state attorneys general offices) to 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 respond to the dynamic nature of mitigating illegal robocalling. K&S 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, K&S 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 S. Mike Kimberling

I, S. Mike Kimberling, President of Advanced Technology Solutions, Inc. ("K&S"), do hereby certify, under penalty of perjury, the following:

- (1) K&S has fully implemented STIR/SHAKEN in the IP portions of its network.
- (1) K&S's Business name and primary address are as follows:

218 N Greenwood Ave
Fort Smith AR 72901
- (2) K&S has the following d/b/a name: K&S Computing.
- (3) K&S has not previously used any other business name.
- (4) 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.
- (5) Sumner M Kimberling Jr. is K&S's owners and director. He has not had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (6) K&S's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (7) K&S has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (8) K&S is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (9) K&S's Operating Company Number is 516K.

/S. Mike Kimberling/
S. Mike Kimberling