

Robocall Mitigation Plan

Business Information

KDDI America, Inc.
7 Teleport Drive
Staten Island, NY 10311

Contact Information

Peter C. Kuan
Senior Tax Manager
(971) 488-3602
p.kuan@kddia.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, outlines "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

KDDI America, Inc. ("KDDIA") is dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. As KDDIA lacks control over the necessary infrastructure, it is exempt from STIR/SHAKEN requirements. In compliance with the R&O, KDDIA submits this RMP and certification.

Know Your Customer

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

New Subscribers

All new subscribers go through identity verification protocols through which KDDIA collects the name, phone number, email address, and credit card information from each new subscriber.

Existing Subscribers

KDDIA require updates of subscribers' information on all their orders, if applicable. Each order's information is checked to ensure the account is not compromised and is being used for its intended purpose. The process is the same as the new subscriber process.

Acceptable Use Policy

KDDIA maintains an Acceptable Use Policy ("AUP") that subscribers must agree to before being permitted to use KDDIA's network. Among other things, this 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 KDDIA's service to engage in or in connection with fraudulent activities. KDDIA's terms with subscribers specify that KDDIA may take action up to suspension or termination of service for violation of the AUP.

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, KDDIA provides the following information concerning its upstream voice carriers.

KDDIA receives voice traffic from the following upstream providers:

AT&T
208 S. Akard St.
Dallas, TX 75202
Lucy Merkle
Im8354@att.com

Verizon
1 Verizon Way
Basking Ridge, NJ 07920
Janbec Chataw
janbec.chataw@verizonwireless.com

These upstream providers abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to KDDIA. The parties do not have a provision in their

service contract concerning robocalls, but KDDIA and its upstream providers work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Analytics for Monitoring Traffic

KDDIA works with its upstream carriers to analyze high-volume voice traffic to identify and monitor patterns consistent with robocalls. If a calling pattern is detected that is consistent with illegal robocalls, KDDIA and its upstream providers will identify the party that is using its network to transmit 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.

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

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, KDDIA and its upstream providers work together to follow procedures on investigating such subscribers. The procedures 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.

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

Blocking

KDDIA works with its upstream carrier to implement Do Not Originate requests it receives from the ITG. KDDIA will cooperate with Investigative Bodies, including law enforcement, state attorneys general offices, 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. KDDIA 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, KDDIA 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 Peter C. Kuan

I, Peter C. Kuan, Senior Tax Director of KDDIA America, Inc. ("KDDIA") do hereby certify, under penalty of perjury, the following:

- a. KDDIA is exempt from the Commission's requirement to implement STIR/SHAKEN in the IP portions of its network, as it lacks control over the necessary infrastructure
- b. KDDIA's business name and primary address are as follows:

KDDI America, Inc.
7 Teleport Drive
Staten Island, NY 10311

- c. Entities that own 10% or more of KDDIA are: KDDIA Corporation, which owns 100% of KDDIA. KDDIA has no affiliates or subsidiaries.
- d. None of the entities listed above have had licenses revoked by the FCC or have been subject to FCC enforcement actions.
- e. KDDIA does not have any other business name.
- f. KDDIA has not previously used any other business name.
- g. 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.
- h. KDDIA's role in the call chain is that of a voice service provider without a STIR/SHAKEN implementation obligation to serve end-users.
- i. KDDIA has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- j. KDDIA is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- k. KDDIA is not required to, nor does it have, and Operator Code Number.

/s/ Peter C. Kuan