

Robocall Mitigation Plan

Business Information

IronEdge Group, Ltd
16285 Park Ten Place
Suite 150
Houston, TX 77084

Contact Information

Fred Forston
Systems Engineer III, VoIP
773-574-5555
accounting@ironedgegroup.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 (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

IronEdge Group Ltd. is a reseller of VoIP services and is dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network where possible. IronEdge Group Ltd. is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. Because IronEdge Group Ltd. does not have access to the necessary infrastructure, it is not required to be STIR/SHAKEN compliant. IronEdge Group, Ltd. 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 IronEdge and its partner in which our partner transmits, originates, and/or terminates calls based on behalf of the subscriber.

IronEdge Group, Ltd.'s 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, and authorized representative info). Moreover, IronEdge Group, Ltd. accept payments only through approved billing methods (e.g., credit card, ACH, wire transfer). IronEdge

Group, Ltd. periodically review and update 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, IronEdge Group, Ltd. provides the following information concerning its upstream voice service carriers:

Altigen Communications, Inc.
39899 Balentine Drive
Suite 112
Newark, CA 94560
(669) 777-4109
sthompson@altigen.com

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

Analytics for Monitoring Traffic

IronEdge Group, Ltd. works with its upstream carriers to analyze high-volume voice traffic in order to identify and monitor patterns consistent with robocalls. If IronEdge Group, Ltd. 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.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, IronEdge Group, Ltd. 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.

IronEdge Group, Ltd. works with its upstream providers to investigate suspicious activity found by the carriers' monitoring systems or reported to IronEdge Group, Ltd. by subscribers or third parties. An investigation could potentially result in opening a traceback request or with IronEdge Group, Ltd. 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. IronEdge Group, Ltd. certifies that it will respond to all traceback requests within 24 hours of

receiving same.

Blocking

IronEdge Group, Ltd. will implement Do Not Originate requests it receives from the ITG. IronEdge Group, Ltd. 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, IronEdge Group, Ltd. will take appropriate action which may include suspending or terminating the subscriber's use of IronEdge Group, Ltd.'s network and utilizing service restriction blocks. IronEdge Group, Ltd. 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. IronEdge Group, Ltd. 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, IronEdge Group, Ltd. 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.