

Robocall Mitigation Plan

Business Information

Intergo Telecom Ltd
1717 N ST NW
Ste 1
Washington, DC 20036

Contact Information

Marios Italos
CEO
813-212-4306
italosm@intergotelecom.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

Intergo Telecom Ltd ("Intergo Telecom") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. Intergo Telecom has fully implemented STIR/SHAKEN. In compliance with the R&O, Intergo Telecom 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 Intergo Telecom in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

There are limitations on the number of simultaneous calls customers can make as per their use case. Customers can only use Caller ID's for numbers we supplied.

All new subscribers go through sign up process and during the account registration process. Intergo Telecom confirms an account by vetting a subscriber directly. The vetting process includes collecting information such as:

- physical business location;
- business contact information;
- contact person(s) details;
- valid 3DS Passed payment method; and
- limitations on the number of simultaneous calls a subscriber can make.

Acceptable Use Policy

Intergo Telecom maintains an Acceptable Use Policy ("AUP") that subscribers must sign before being permitted to use Intergo Telecom's network. Intergo Telecom prohibits the use of the services or the network for any illegal activity, high-risk use, infringing activity, malicious activity, objectionable activity, misrepresenting origin and/or identity, unsolicited communications, spam, bulk messages, excessive or unauthorized use, circumventing compliance or security, or interception. Among other activities, the AUP prohibits the following:

- Spamming or sending unsolicited messages, such as bulk emails or SMS messages, without the recipient's consent.
- Engaging in any fraudulent or malicious activities, such as phishing scams, hacking, or spreading viruses or malware.
- Using the Telxi Services to violate intellectual property rights, such as pirating copyrighted content or distributing counterfeit goods.
- Engaging in any form of harassment, such as cyberbullying or sending threatening or offensive messages.
- Misrepresenting oneself or the origin of a communication, such as spoofing caller ID or forging email headers.
- Interfering with or disrupting the Telxi network or the networks of other users, such as through denial-of-service attacks or other forms of network congestion.
- Collecting personal information about others without their consent or using such information for malicious purposes.

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

- 1) Inteliquent, Inc. DBA Onvoy, Sinch
550 W. Adams St.
Suite 900
Chicago IL 60661

Stacy Graham
Director, Assurance & Trust Services
217-862-1953
stacy.graham@sinch.com

- 2) Third Base International Telecom LLC DBA TBI Telecom
3949 Evans Ave -Ste 301B
Fort Myers FL 33901
Mark Saccente Sr
239-935-7286
mark@tbitelecom.com

Interco Telecom has contractual provisions with its upstream carriers concerning robocall mitigation, and Interco Telecom and its upstream providers work together to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Telephone Number Authorization

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 Interco Telecom and/or obtained by Interco Telecom from Interco Telecom's underlying carriers for use by the subscriber. In most cases, Interco Telecom directly manages the TNs used by its subscribers. Interco Telecom tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Interco Telecom's assignment of the TN to its subscriber.

If a subscriber wishes to use a TN as a caller identity and that TN is not directly managed by Interco Telecom, then TN validation is necessary. If a subscriber's end-user can provide a valid letter of authorization that they are the authorized user of such TNs, Interco Telecom will attest calls originated with these TNs.

When originating a call, Interco Telecom checks the calling party number against Interco Telecom's inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

During Service

All subscribers can report any suspicious call connected through their account and measures are set to prevent future calls from/to that individual numbers for all subscribers (none routed by the platform from that moment on - blacklisting). These features are:

- VoIP originated calls are signed with subscriber caller ID only after number validation; and
- Requiring authentication to initiate any call, or a whitelist of originating numbers that is under customer's control.

Monitor Traffic with Analytics

Interco Telecom has an in-house analytics team that monitors the subscriber's phone logs when we suspect traffic abnormalities. On its network, Interco Telecom strictly prohibits robocalls and clearly communicate this to all users. If suspicious call activity is detected, we swiftly investigate, and

terminate the user from our network permanently to prevent unauthorized use. We're committed to maintaining a secure and compliant telecommunications environment.

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

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.

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.

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

Interco Telecom will investigate suspicious activity reported to Interco Telecom by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Interco Telecom contacting a subscriber to correct improper use of the platform, or, if the subscriber does not respond or comply, to block their use of the platform.

For all new and renegotiated Interco Telecom contracts governing the transport of voice calls, Interco Telecom will use best efforts to contractually require Interco Telecom's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Interco Telecom will implement Do Not Originate requests it receives from ITG. Interco Telecom has mechanisms to automatically block suspicious calls using internal analytics at the switch level. If Interco Telecom identifies suspected robocalling patterns that are confirmed with further investigation, Interco Telecom will take appropriate action which may include suspending or terminating the subscriber's use of Interco Telecom's network. Interco Telecom 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), the FCC, and 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. Interco Telecom 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, Intergo Telecom 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 Marios Italos

I, Marios Italos, CEO of Intergo Telecom Ltd ("Intergo Telecom") do hereby certify, under penalty of perjury, the following:

- a. Intergo Telecom has fully implemented STIR/SHAKEN in the IP portions of its network.
- b. Intergo Telecom's business name and primary address are as follows:

Intergo Telecom Ltd.
1717 N ST NW
Ste 1
Washington, DC 20036

- c. Intergo Telecom has no other business names in use.
- d. Intergo Telecom has not previously used any other business name.
- e. 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.
- f. Intergo Telecom has the following parent company: Intergo Interactive Ltd.
- g. Intergo Telecom's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- h. Intergo Telecom and its parent company have not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- i. Intergo Telecom and its parent company have not subject been to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- j. Intergo Telecom's Operator Code Number is 592K.

Marios Italos

Marios Italos