

Robocall Mitigation Plan

Business Information

Sentry IT Solutions LLC
60 Bethpage Rd
Hicksville NY 11801

Contact Information

Alexander Yfraimov
Partner
5163860588
alexey@sentrymsp.com

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

Sentry IT Solutions LLC ("Sentry") is a small VSP dedicated to stopping illegal calls from traversing our network and monitoring the calls coming into our network. Sentry is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, Sentry was previously exempt from the FCC's STIR/SHAKEN rules. The R&O requires that pure resellers such as Sentry now file RMPs. This document delineates Sentry's RMP. Because Sentry does not have access to the necessary infrastructure, it relies on its upstream carrier to assist in robocall mitigation. As delineated herein, Sentry works closely with its upstream provider to carry out the required mitigation functions.

Know Your Customer ("KYC")

We are a small business and deal with other small businesses. Before bringing on a new customer we inquire about the specifics of their business to get a better understanding of the manner they will be using their VOIP system.

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

We set restrictions on the amount and frequency of payments to prevent money laundering and fraudulent activities.

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

- physical business location;
- contact person(s);
- phone number;
- email address;
- nature of the customer's business.

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, Sentry provides the following information concerning its upstream voice service carrier.

Sentry has one upstream provider from which it receives voice traffic:

Skye Telecom LLC d/b/a Skyetel
915 Broadway St #100
Vancouver, WA 98660
Joshua Riffle
noc@skyetel.com

Sentry actively cooperates with its upstream provider, which fully implements STIR/SHAKEN. Sentry 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")

Sentry maintains an AUP that subscribers must sign before being permitted to use Sentry'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 local, state, or federal law;
- violating applicable industry accepted guidelines; and
- using Sentry's service to engage in or in connection with fraudulent activities.

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

Mitigation During Service

Sentry works with its upstream provider to ensure that 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. 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.

Analytics for Monitoring Traffic

Sentry works with its upstream provider to identify behaviors which indicate illegal call activity. 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).

Investigate Suspicious Activity

We are keeping a detailed call log which we will examine in the event suspicious activity takes place.

When traffic analysis indicates the presence of likely illegal robocalling, Sentry works with its upstream provider to follow 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.

Because Sentry does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in Sentry's analytics.

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

Sentry works with its upstream provider to investigate suspicious activity found by the carrier's monitoring systems or reported to Sentry by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Sentry 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 to block their use of the platform.

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

Blocking

Sentry will implement Do Not Originate requests it receives from the ITG.

Sentry's upstream provider would alert Sentry if one of Sentry's clients is placing a large volume of calls simultaneously, which is a common sign that a VOIP system is compromised. That way, Sentry can rapidly take action, investigate and block any further calls manually. Skyetel also has analytics to block suspicious inbound calls.

If Sentry and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, Sentry will take appropriate action which may include suspending or terminating the subscriber's use of Sentry's service. Sentry 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), 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. Sentry 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, Sentry 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 Alexander Yfraimov

I, Alexander Yfraimov, Partner of Sentry IT Solutions LLC ("Sentry"), do hereby certify, under penalty of perjury, the following:

- (1) Sentry, 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) Sentry 's Business name and primary address are as follows:

Sentry IT Solutions LLC
60 Bethpage Rd
Hicksville NY 11801
- (3) Sentry has no other business names in use.
- (4) Sentry has not previously used any other business name.
- (5) The following persons own more than 10% of Sentry each: Alexander Yfraimov, Brian Spinner, Elaine Spinner. None of these persons have had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (6) 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.
- (7) Sentry's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (8) Sentry has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (9) Sentry is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (10) Sentry is not required to have, and does not have an operating company number.

/ Alexander Yfraimov/
Alexander Yfraimov