

Robocall Mitigation Plan

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

Talbit INC, LLC ("Talbit INC"), is a small VSP dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network. As certified in the FCC's Robocall Mitigation Database, Talbit INC has fully implemented STIR/SHAKEN. In compliance with the R&O, Talbit INC submits this RMP and certification.

Know Your Customer ("KYC")

Before any client is allowed to place outbound calls, we have them complete a Know Your Customer form, which tracks items as such IP, MNC for cell phones, and others. Once a client, our STIR/SHAKEN software checks the requesting and media IPs and will change the attestation level based on those parameters. If an international media IP is detected, we may update the attestation level to a C. We also have developed in-house tools to help provide a likelihood of suspicious traffic. All new Talbit INC subscribers must provide:

1. Company name and Address
3. Contact name and Number
5. Incorporation date
6. EIN (IRS Notice CP 575)
8. DBA
9. Web domain
10. Industry (Goods/services)
12. 499a Filed ID

New subscribers have their outbound calls rate-limited to one per second, and human contact via phone call or in-person is required in order to increase that rate. New subscribers placing

outbound calls can only use Caller IDs which have been purchased through our platform or ones validated through automated-number-validation voice call. All pay-by-card subscribers have limits placed on the number of payments they may make per day and the size of those payments. Both are kept low unless we have had human contact with the customer via phone call or in-person. Pay-by-invoice is allowed only for subscribers who we know well, with human contact via phone call or in-person at the very least, and credit and associated checks having taken place.

Talbit INC is a small company, we have a small number of customers. We know our customers and understand their use cases.

Know Your Upstream Providers

In accordance with the Commission's directive in Advanced Methods to Target and Eliminate. Talbit INC 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")

Talbit INC maintains an AUP that subscribers must agree to before being permitted to use its software and services. Among other things, the AUP prohibits:

Using our service for any illegal purposes whatsoever;

Engaging in activity for which FCC or any equivalent national regulatory authority, has Restricted or regulated in relation to proper use of the public telephony network or the Internet; Using our service if Talbit INC determines, at its sole discretion, that its provision for this Customer is prohibited by applicable law or has become impractical or unfeasible for any legal or regulatory reason; and using our service to offer or otherwise make available to others fraudulent goods, services, schemes, or promotions, including make-money-fast schemes, Ponzi and pyramid schemes, phishing, pharming, harvesting or similar deceptive practices.

Analytics for Monitoring Traffic

Talbit INC 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.

We use in-house and SIPNAV's Roboguard technologies for traffic analytics.
Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Talbit INC's 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 or her particular use case and validate that the activity belongs to that subscriber.

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

If a traceback request is sent to us, we suspend the client, investigate, and send the information back to ITG. Talbit INC commits to responding within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Blocking

Talbit INC will promptly respond to Do Not Originate requests it receives from the ITG. Talbit INC has mechanisms to automatically block suspicious calls using internal analytics. If Talbit INC’s monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Talbit INC will take appropriate action which may include suspending or terminating the subscriber’s use of Talbit INC’s network. Talbit INC will cooperate with investigative bodies (provide a single point of contact to address traceback requests from law enforcement including state attorneys general offices), to the FCC, and/or the ITG; as well as documenting requests and 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. Talbit INC 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, Talbit INC 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