



Robocall Mitigation Plan (RMP)

Definitive Technology Solutions
9401 James Ave S, Ste 162
Bloomington, MN 55431

Contact Information

Tammy Brandt
Director of Human Resources
952-516-7900
tbrandt@go-dts.com

Overview

Consistent with the expanded robocall mitigation obligations adopted in the Sixth Caller ID Authentication Report and Order, this RMP has been amended to include the following, as it pertains to the "know your upstream carrier" as well as new, and renewing customers;

1. A Description of how DTS is meeting its existing obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls;
2. A description of our "know-your-upstream provider" procedures in place designed to mitigate illegal robocalls;
3. A description of any call analytics systems we use to identify and block illegal traffic, including whether they use a third-party vendor or vendors and the name of the vendor(s).

This document serves as DTS' RMP. Because DTS does not have access to the necessary infrastructure, it relies on its upstream carrier partners to assist in robocall mitigation. As delineated herein, DTS works closely with its upstream provider to carry out the required mitigation functions. DTS, Inc has upstream providers from which it receives voice traffic:

PayG LLC dba SkySwitch
Arborcrest 1, 751 Arbor Way Suite 150
Blue Bell, PA 19422
Phone: 747.777.8100
Email: support@skyswitch.com

Skye Telecom LLC dba Skyetel
PO Box 2445
Vancouver, WA 98668
Phone: 360.986.5200
Email: noc@skyetel.com



Robocall Mitigation Plan (RMP)

BCM One Cloud Communications LLC, dba Flowroute
295 Madison Avenue, 5th Floor
New York, NY 10017
Phone: 855.356.9768
Email: support@flowroute.com

Purpose

Definitive Technology Solutions, Inc., ("DTS"), (the "Company") is committed to cooperating with the Federal Communications Commission (FCC), law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that it learns are using our service to originate calls or transit calls into the United States and territories.

DTS' FRN Number is 0034706614.

DTS' role in the call chain is that of a voice service provider, and has fully implemented Stir/Shaken.

DTS has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.

The Company commits to fully responding within 24 hours to all traceback requests from the ITG, the TPTG, the FCC, and law enforcement. The Company shall cooperate with these groups to investigate and stop any illegal robocallers from using Company's services to carry or process illegal calls. When notified by the FCC's Enforcement Bureau, Company shall block and report identified illegal traffic, and any substantially similar traffic, on an ongoing basis (unless Company's investigation determines that the traffic is not illegal) when Company receives actual written notice of such traffic from the Enforcement Bureau. If Company determines that the identified traffic is not illegal, Company shall provide the Enforcement Bureau with an explanation as to why Company reasonably concluded that the identified traffic is not illegal, and what steps it took to reach that conclusion.

The Company utilizes a combination of internal tools and third-party solutions to check for Do Not Originate (DNO) numbers. In addition, the Company utilizes a combination of internal tools and third-party solutions to detect invalid phone number formats, area codes and unassigned number blocks. The Company also utilizes data analytics to detect and investigate irregular and unexpected calling patterns, originating number use against customer profiles.

The Company uses data systems for analytics and reviews to identify illegal robocalling, in addition to a Know Your Customer (KYC) requirement to access the Company's networks. The process includes:

- Monitoring the network to identify suspicious traffic patterns.
- Limiting customers' capacity via call per second and/or concurrent session limits.
- Regularly checking call patterns for possible abusive traffic.



- All new customers are verified with a combination of electronic and manual verification systems, credit reviews, references from trusted industry members, and previous experiences with customer executives and employees. The Company severely limits the capabilities of new accounts until these appropriate processes are complete.

Know Your Customer

Identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity, that is associated with that subscriber. A subscriber is an entity that has a business relationship with DTS in which we transmit calls based on behalf of the subscriber by reselling SIP services purchased from our upstream provider.

As such, all new subscribers have their identity confirmed by DTS by verifying the subscriber's name, email address, credit card information, and contact phone number. All new subscriber activity is monitored via a third-party PBX monitoring solution, as well as with tools provided by our upstream service provider, which are further detailed below.

Existing subscribers have been validated via account updates where each subscriber's identity was verified again to ensure the account is not compromised and is being used solely for its intended purpose.

Acceptable Use Policy

DTS maintains an Acceptable Use Policy ("AUP") that subscribers must agree to before being permitted to originate or terminate calls on DTS 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 DTS' services to engage in or in connection with fraudulent activities.

DTS' AUP specifies that DTS may act appropriately, including suspension or termination of service, for violations of same. The Company reserves the right to refuse traffic from any party, at any time, where robocalling or use of originating numbers that are not valid or they are not authorized to use, has occurred or is suspected. The Company is able to block the originating number(s), terminating numbers(s), trunk(s) or customer, including termination of customer relationship, invalid originating number(s) or spoofed origination number(s) transiting the Company's networks, to prevent robocalling.

Mitigation During Service

DTS 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 (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 via SMS; and



- customer authentication to initiate any call, or a whitelist of originating numbers that is under customer's control.

Analytics for Monitoring Traffic

DTS works with its upstream providers 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 initiated 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 and Traceback Requests

When traffic analysis indicates the presence of likely illegal robocalling, DTS works with its upstream provider to follow defined procedures on investigating such subscribers.

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

Pursuant to 47 CFR § 64.6305(B)(4), DTS has designated a point of contact to receive notice of any incidents of illegal robocall traffic. This person's name, title, address, phone number, and email address are in the Robocall Mitigation Database portal.

This individual will be the main contact responding to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. DTS will respond fully and within 24 hours to traceback requests from such entities, as well as its upstream provider, and will cooperate in investigating and stopping any illegal robocalls that attempt to use its network or services to originate calls.

Telephone Validation Process

A subscriber is permitted to use a telephone number as their caller identity, if a number is directly managed by DTS and/or obtained by DTS via an upstream provider. DTS and/or its upstream provider has established processes for ensuring subscribers are utilizing only telephone numbers assigned to them or have been authorized for use. DTS and/or its upstream provider screens all originating calls and only allows the call to be connected if the originating telephone number matches one of the assigned numbers for the subscriber.

Blocking

DTS will implement Do Not Originate requests it receives from the ITG. DTS' upstream provider has mechanisms to automatically block suspicious calls using internal analytics. If DTS and/or its upstream carrier



Robocall Mitigation Plan (RMP)

identifies suspected robocalling patterns that are confirmed with further investigation, DTS will take appropriate action which may include suspending or terminating the subscriber's use of DTS services. DTS 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.



Robocall Mitigation Plan (RMP)

Certification

I, Gordon Running, President and COO for Definitive Technology Solutions, Inc, do hereby certify, under penalty of perjury, the following:

(1) Definitive Technology Solutions, Inc, ("DTS"), by virtue of its status as a "pure reseller" does not have the access to the necessary infrastructure to implement STIR/SHAKEN, and therefore has not implemented STIR/SHAKEN in the IP portions of its network.

(2) DTS' Business name and primary address are as follows:

Definitive Technology Solutions, Inc.
9401 James Ave S, Ste 162
Bloomington, MN 55431

(3) DTS has no other business names in use.

(4) DTS has not previously used any other business name.

(5) 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.

(6) DTS' role in the call chain is that of a voice service provider, that has fully implemented STIR/SHAKEN..

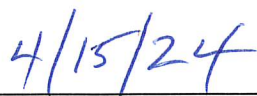
(7) DTS has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.

(8) DTS is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

(9) DTS is not required to, and does not have, an operator company number.



Gordon Running, President and COO



Date