



## Robocall Mitigation Plan

Dynalink Communications, Inc. 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.

We are a reseller of Bulk Solutions, LLC (RMD0001449), (referred to below as: "The Company or Company"), and do not have the capability to implement STIR/SHAKEN. Bulk Solutions has implemented STIR/SHAKEN protocols in their IP Voice networks.

We have not been prohibited from filing a certification in the Robocall Mitigation Database.

Dynalink, nor any of our executives or principals have a history of enforcement actions for illegal robocalls, TCPA or TSR violations or related state law violations.

We use the affirmative and effective measures detailed below to prevent the origination or transit of illegal robocalls.

### Know Your Customer

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

### Traceback

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls.

### Robocall Mitigation Program

We use software provided by **Bulk Solutions (RMD0001449)** to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls.

### Bulk Solutions Robocall Mitigation Solution Overview

- General information
  - Robocall scoring is based on the annual +100B carrier calls that Bulk Solutions processes as part of the Caller Name service.
  - STIR/SHAKEN Transaction Detail Records (TDRs) are now being added as an additional data source.

- Each call is assessed through the Bulk Solutions model, leading to constantly refreshed view of call behavior and probability of a given number currently being used for robocalling.
  - Active numbers are assessed by the model for behavioral attributes typically associated with robocalling including:
    - Neighbor spoofing events
    - Sudden spikes in volume, such as driven by call spoofing
  - Do-Not-Originate (DNO) numbers are also deemed to be robocalls if they are the calling party number. This is sourced from industry (e.g., US Telecom) and directly from enterprises.
  - The service covers both US domestic and international TNs.
- Calls originating from our network (i.e., Robocall Protection)
    - Provides detailed reporting identifying suspected illegal robocalls and alerts if calls originate where the calling number is invalid, unallocated, on a Do-Not-Originate list.
    - If the platform detects a suspected robocalling patterns Dynalink will take appropriate action which may include suspending or terminating the subscriber.
    - Supports a real time query to service to determine if a number originating on your network could be a robocall. Such calls can be blocked, or the terminating party can be notified via CNAM.
    - For each new instance of robocalling using the Operating Service Provider (OSP)TNs, an alert is sent to the OSP in near real time. This alert will result in the OSP (manually) blocking the TN and all TSPs being alerted via CNAM, through an overlay such as “ROBOCALLER”. The CNAM alerting helps address instances of spoofing of TNs that are not going through the OSP that owns the number.
  - Termination (i.e., Robocall Mitigation)
    - Supports a real-time query to service to determine if a number terminating on your network could be a robocall. This protects subscribers from calls that come from networks that cannot authoritatively attest to the end user caller (i.e., all Communications Service Providers (CSPs)that do not have STIR/SHAKEN and all CSPs with STIR/SHAKEN, but who do not have a direct and vetted end user relationship.)
    - Such calls can be blocked or the called party can be notified via CNAM.

In addition, we have implemented a Call Abuse Policy and have published the following policy to our web site, terms of use, and have notified our customers of the policy as copied below:

*“Any call originated on the **Dynalink Communications’** network is subject to inspection and investigation if the call is suspected of being fraudulent, abusive, or illegal. Calls meeting any of these criteria will be blocked. If these conditions are repeated, becoming excessive, the subscriber may be disconnected from **Dynalink Communications’** network, may be subject to further investigation by the FCC for enforcement of the TRACED Act and the subscriber may be subject to fines and penalties imposed by the FCC or the jurisdictional court.”*