

DeansList Robocall Mitigation Plan

Business Information

DeansList Inc
PO Box 887
South Orange, NJ 07079

Contact for Robocall Mitigation Related Issues

DeansList will update our Robocall Mitigation filings within 10 days of any changes to the information outlined in the plan.

Please direct any questions related to mitigation issues to:

Matthew Robins

matt@deanslistsoftware.com

646.759.8801

Overview

This Robocall Mitigation Plan is submitted on behalf of DeansList Inc (DeansList). DeansList is a US-based SaaS provider of operational software K-12 schools, school districts, and non profit organizations. A component of DeansList's software is a communication tool that allows school employees, including teachers and administrators, to send robocalls to school employees and families of students. Educators use the communication tool to share information such as: announcements, reminders, school closures, etc. DeansList uses a third party provider distribution/placement of the SaaS-originated voice calls.

Know Your Underlying Provider

DeansList delivers calls via two known, reputable downstream voice providers Plivo and Bandwidth. Both providers have implemented STIR/SHAKEN and sign all calls where the originating phone number is either rented from them, or has been verified to belong to our registered client. Both Plivo and Bandwidth have agreed to abide by the FCC's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice services to DeansList. DeansList and our providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Know Your Customer/ Customer Due Diligence

DeansList conducts due diligence on all new and renewing clients. As a small provider, DeansList maintains close contact with each client using voice services. Each client's information, including school or school organization address and employee identities, is verified at time of purchase and renewal. All DeansList users are verified employees of schools, school districts, or nonprofit organizations. DeansList enforces terms of service and privacy policies which define

circumstances under which it can suspend, deny or terminate services to a customer. DeansList's Terms of Service prohibit usage of our platform for marketing activities or any non-school related business including illegal robocalling.

Responding to Traceback Requests

Working in conjunction with our voice call provider(s), DeansList is committed to respond fully, within 24 hours, to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that use DeansList to originate, carry, or process illegal robocalls. If a traceback exposes an existing client as the source of fraudulent robocalls a demand for explanation and verification of mitigation will be issued to the client. If the fraudulent traffic is not mitigated, DeansList will suspend service for the offending client.

DeansList has a designated individual as a dedicated point of contact for addressing traceback requests - Matthew Robins, matt@deanslistsoftware.com, 646.759.8801, as well as a backup on-call representative available at tech@deanslistsoftware.com.

International Calling

DeansList is not currently an international voice services provider. If at any time DeansList does decide to sell our services to international customers using North American Numbering Plan resources, we will familiarize ourselves with and develop best practices for full vetting of such customers and work with our underlying provider(s) to perform the necessary telephone number validation on all international originated calls.

Call Analytics

DeansList relies on its upstream providers to analyze traffic and determine if traffic should be blocked best on its best practice. This model has been successfully used to mitigate fraudulent calling as it is detected by our upstream provider and then they notify us of the abuse.

Ongoing Robocall Mitigation + Preventing/Avoiding Illegal Robocall Origination

DeansList's software is designed to both mitigate the potential for illegal robocalling, as well as to identify and quickly mitigate any suspected robocalling. DeansList users are limited to dispatching calls to numbers associated with a student's parents/guardians according to official school records. Users may not send calls to additional numbers not associated with an enrolled student. All call records are saved and visible to school administrators, including sender name, email address and date/time, so any illegal or unauthorized use of call features would be immediately identifiable to a user's supervisors.

Additionally, DeansList monitors and examines call detail records (CDRs) to detect suspicious call activity and/or calling patterns. When we and/or our underlying provider detect network usage patterns consistent with illegal robocalls or suspect illegal robocalling is taking place, we will immediately seek to identify the party that is originating, terminating, or routing these calls so that we may take appropriate action. The actions taken may include, but are not limited to initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate and/or dba name; block the party's ability to originate, terminate, or route calls on the network; and/or providing notice to law enforcement authorities.

As part of our Plan to mitigate and prevent any originating robocalls, we are committed to early identification and investigation of possible robocalling conditions. Among other things, we watch for higher-than-normal call volume, including large bursts of traffic in small timeframes or traffic volumes deemed excessive based on the number of students enrolled at a school.

In the event that DeansList discovers a customer is originating illegal robocalls we will suspend services to either the offending user or the entire client until the client can demonstrate that the issue has been remedied.