



UNDERSTAND. DELIVER. IMPROVE.



ROBOCALL Mitigation Policy

Damovo USA Inc.

FRN: 0033678566

April 2023

Contents.

1.1	Document Control	2
1.2	Overview.....	3
1.3	General Prohibition Against Illegal Robocalling	3
1.4	Know Your Customer & Technical Limitations.....	3
1.5	Network Monitoring	3
1.1	Traceback and Enforcement Cooperation	3

1.1 Document Control

Document Author	Version	Release Date	Status	Comment
Dan Unwin	1	04/19/2023		Initial Document Creation

1.2 Overview

The FCC requires that all telecommunications register their details against the the Robocall Mitigation Database (RMD) their status for compliance with STIR/SHAKEN. Those not fully compliant must implement and certify to the implementation of a Robocal Mitigation Plan (RMP) to ensure that this traffic does not originate on their networks as they work within the industry to become fully compliant.

The Commission requires voice service providers (VSP) to develop a RMP that:

- A. Details the reasonable steps taken to avoid originating illegal robocalls
- B. Demonstrates a commitment to respond to traceback requests to cooperate with investigating and stopping illegal robocalls
- C. Is filed in the RMD

This mitigation plan is submitted on behalf of Damovo USA Inc. (Damovo).

Damovo provides managed voice services to larger enterprises, predominately in Insurance and Manufacturing sectors. Damovo partners with trusted providers to implement STIR/SHAKEN in all of its networks.

1.3 General Prohibition Against Illegal Robocalling

Damovo end users are subject to technical and contractual limitations to prevent activities normally associated with Robocalling including, but not limited to providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call; violating any local, state, or federal law; otherwise using Damovo services in connection with any fraudulent activities.

1.4 Know Your Customer & Technical Limitations

Damovo utilizes a mitigation technique of “Know Your Customer.” Damovo maintains a close relationship with each of our clients and the Brands that they are part of. Generally, each of these clients are large organisations that will not be utilising practices such as ROBOCALL.

Damovo will incorporate contractual terms to ensure customers agree not to utilise prohibited technologies.

Damovo will review customer calling patterns to identify such activity if it is suspected.

Technical limitations are in place as well. Customers do not have direct access to SIP endpoints nor have the ability to perform any outbound calls over our network without utilizing applications such as MS Teams and Contact Centre clients. The technology provided to our clients limits activity to one-to-one communications.

1.5 Network Monitoring

Damovo monitors all outbound calls generated over its networks and highlights any activity indicative of Robocalling. Damovo has an alert set to proactively notify our 24x7 Global Network Operations Centres of suspiciously high volume of calls originating from any of the numbers that we provide to our clients.

1.1 Traceback and Enforcement Cooperation

Damovo will actively cooperate with the traceback community including the FCC, local, state and federal law enforcement, and The Industry Traceback Group (ITG) to investigate and stop illegal robocalls.

Damovo will dedicate resources to provide prompt and complete responses to traceback requests.