



Robocall Mitigation Program (RMP)

0.0 Front Matter

0.1 Record of Revisions

Revision	Date	Author
Reissue	2026-04-15	Robert Nichols (robert.nichols@dialwave.com)

0.2 List of Effective Pages

Chapter 0: Front Matter

Section	Revision	Date
0.1	Reissue	2026-04-15
0.2	Reissue	2026-04-15
0.3	Reissue	2026-04-15

Chapter 1: Introduction

Section	Revision	Date
1.1	Reissue	2026-04-15

Chapter 2: Robocall Mitigation Program (RMP)

Section	Revision	Date
2.1	Reissue	2026-04-15
2.2	Reissue	2026-04-15
2.3	Reissue	2026-04-15

0.3 Table of Contents

Chapter 0: Front Matter 0.1-1

0.1 Record of Revisions 0.1-1

0.2 List of Effective Pages 0.2-1

0.3 Table of Contents 1.1-1

Chapter 1: Introduction 1.1-1

1.1 Overview 1.1-1

1.1.1 Mission 1.1-1

1.1.2 Responsibility and Authority 1.1-1

Chapter 2: Robocall Mitigation Program (RMP) 2.1-1

2.1 Policies and Procedures 2.1-1

2.1.1 Robocall Mitigation Policies 2.1-1

2.1.2 Robocall Mitigation Procedures 2.1-1

2.2 Compliance 2.2-1

2.2.1 STIR/SHAKEN Implementation 2.2-1

2.2.2 TRACED Act Compliance 2.2-1

2.3 Training 2.3-1

2.3.1 Required Training 2.3-1

1.0 Introduction

1.1 Overview

1.1.1 Mission

Pursuant to the applicable orders and regulations of the Federal Communications Commission (FCC), the following Robocall Mitigation Program (RMP) details the policies and practices that Dialwave, Inc. (Dialwave) has established to prevent unlawful robocalls from originating on, terminating to, or routing through Dialwave's voice networks.

1.1.2 Responsibility and Authority

The VP, Operations is responsible for the content of this document and has the authority to make changes.

2.0 Robocall Mitigation Program (RMP)

2.1 Policies and Procedures

2.1.1 Robocall Mitigation Policies

[47 CFR 64.6305(a)(1)]

Dialwave has implemented the following policies to mitigate robocalls:

- a. Prior to accepting traffic from a customer, Dialwave will verify the legitimacy of the customer and ensure compliance with regulatory obligations. This includes the implementation of robust Know Your Customer (KYC) procedures for onboarding and renewing all customers. Customers are required to provide detailed information, including:
 - a. Legal name of the company and any d/b/a or trade names.
 - b. State or country of incorporation or organization.
 - c. Physical business address that reflects the true operational location. Virtual addresses, shared office locations without a dedicated suite or floor, P.O. boxes, and mail forwarding services are not sufficient as a physical address.
 - d. Billing name and address, if different.
 - e. Primary business contact name, title, email address, and telephone number.
 - f. Alternate telephone number for the customer.
 - g. Government-issued identification number and, where applicable, Federal Tax ID or equivalent business registration number.
 - h. Description of the business, services offered, target customers, and intended use of Dialwave services.
 - i. Expected traffic profile, including product types, originating and destination markets, caller ID practices, expected volumes, and whether traffic is domestic, international, wholesale, enterprise, A2P, or other.

If the customer operates as a Voice Service Provider, Foreign Voice Service Provider, Intermediate Provider, or Gateway Provider, Dialwave will verify that the entity is listed in the FCC's Robocall Mitigation Database (RMD) and has not been removed due to an enforcement action before accepting any traffic. Dialwave will not accept traffic from any provider required to be listed in the RMD that is not listed or has been removed.

- b. Dialwave monitors traffic patterns for unusual activity that may indicate robocall activity.
- c. Dialwave cooperates with law enforcement agencies in investigations related to robocalls.
- d. Dialwave maintains records of all customer interactions related to robocall mitigation.

2.1.2 Robocall Mitigation Procedures

The following procedures are in place to ensure compliance with the RMP:

- a. All employees must report any suspected robocall activity to their supervisor immediately.
- b. Dialwave conducts regular audits of its network to identify and mitigate any potential robocall traffic.
- c. Dialwave maintains a log of all robocall-related incidents and actions taken.

2.2 Compliance

2.2.1 STIR/SHAKEN Implementation

[47 CFR 64.6301(a)]

Dialwave has implemented STIR/SHAKEN technology to authenticate and verify caller identification information. This technology is applied to calls originating from, transiting through, and terminating on Dialwave's network, as applicable and technically feasible. Specifically, Dialwave has the means to:

- a. Authenticate and verify caller identification information for all SIP calls that exclusively transit its own network;
- b. Authenticate caller identification information for all SIP calls it originates and that it will exchange with another voice service provider or intermediate provider and, to the extent technically feasible, transmit that call with authenticated caller identification information to the next voice service provider or intermediate provider in the call path; and
- c. Verify caller identification information for all SIP calls it receives from another voice service provider or intermediate provider which it will terminate and for which the caller identification information has been authenticated.

2.2.2 TRACED Act Compliance

[47 CFR 64.6305(a)(2)]

Dialwave is committed to complying with the TRACED Act, which requires voice service providers to implement measures to prevent unlawful robocalls.

Dialwave will respond within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium. In addition, Dialwave will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. This includes providing call path details, customer information (as permitted by law), and other relevant records to support enforcement actions and to mitigate unlawful traffic.

2.3 Training

2.3.1 Required Training

All employees involved in telecommunications operations must receive training on the RMP. This training ensures that employees understand their responsibilities, including:

- a. Legal requirements;
- b. Know Your Customer (KYC) requirements;
- c. Identifying robocall traffic; and
- d. The necessary protocols for ensuring compliance with regulatory requirements.

Regular updates and refresher courses will be provided to ensure that employees remain knowledgeable about any changes to RMP procedures or applicable laws.