



FRN 001967032

OCN 727K

ROBOCALL MITIGATION PLAN

August, 2026

Table of Contents

I.	Robocall Mitigation Program Introduction	3
A.	Company Summary	3
B.	Filing of RMP and Implementation of STIR/SHAKEN	3
II.	Robocall Mitigation Program	4
1.	Implementing Knowing Your Customer Protocols	5
2.	Implementing Know Your Upstream Provider (KYUP) Protocols	5
3.	Requiring Contractual Provisions to Mitigate Illegal Robocalls	6
4.	Only Accepting Traffic from Providers in the RMD	6
5.	Blocking Calls on a Do-Not-Originate List	7
6.	Analyzing and Monitoring Network Traffic Routing Through DIAL WORLD's Network	7
7.	Ensuring Foreign Providers Are Not Using DIAL WORLD to Carry or Process High-Volume Illegal Traffic onto the U.S. Network	8
8.	Authenticating Voice Traffic	8
9.	Responding to Commission, Law Enforcement and ITG Traceback Requests	9
10.	Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues	9
11.	Training Personnel	10
12.	Updating DIAL WORLD's RMD Submission and RMP and Annual Recertification	10

I. Robocall Mitigation Program Introduction

Pursuant to the applicable orders and regulations of the Federal Communications Commission (“FCC” or “Commission”), the following Robocall Mitigation Program (“RMP”)

details the policies and practices that DIAL WORLD COMMUNICATIONS LLC (“DIAL WORLD”), FRN 001967032 was established to prevent unlawful robocalls from originating on, terminating to, or routing through its voice network where it is operating as a Voice Service Provider, Gateway Provider, or Intermediate Provider. Unless defined differently herein, capitalized terms used herein have the same definitions as set forth under 47 C.F.R § 64.6300.

A. Company Summary

DIAL WORLD COMMUNICATIONS LLC (“DIAL WORLD”) is a global provider of cloud communications and VOIP communications services. Service offered include long distance prepaid calling cards and services as well as domestic and international termination services. As indicated above, depending on the services provided, DIAL WORLD COMMUNICATIONS LLC may serve as a Voice Service Provider, an Intermediate Provider, and/or a Gateway Provider.

B. Filing of RMP and Implementation of STIR/SHAKEN

DIAL WORLD has fully implemented STIR/SHAKEN and has submitted its certification that all voice traffic that originates on its network is authenticated with STIR/SHAKEN consistent with 47 C.F.R. § 64.6301(a). In accordance with the RMD 12/2022 Filing Instructions¹, FCC Rule 47 C.F.R. § 64.6305(b) and because DIAL WORLD is a provider that performs more than one role in the call path, DIAL WORLD has certified in the Robocall Mitigation Database, and has fully implemented the STIR/SHAKEN authentication framework across its network consistent with 47 C.F.R. §§ 64.6301 and 64.6302, that it has a STIR/SHAKEN obligation in each of the roles it performs, namely: (i) as a Voice Service Provider with a STIR/SHAKEN obligation acting as a wholesale provider originating calls and serving end-users; (ii) as a Gateway Provider with a STIR/SHAKEN obligation; and (iii) as a Non-Gateway Intermediate Provider with a STIR/SHAKEN obligation. In addition, DIAL WORLD has uploaded this RMP into the RMD because it “details the specific reasonable steps it has taken to avoid carrying or processing illegal robocall traffic” and has included “a commitment to respond fully and 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 any illegal robocallers that use its service to carry or process calls².”

¹ See Robocall Mitigation Database External Filing Instructions, Version: December 2022 (“RMD 12/2022 Filing Instructions”), available at <https://www.fcc.gov/sites/default/files/rmd-instructions.pdf>.

² RMD 12/2022 Filing Instructions at 12-13. See also 47 C.F.R. § 64.6305(d)(2)(ii) (even if a gateway provider is fully compliant with STIR/SHAKEN, it must file an RMP that sets forth “[t]he specific reasonable steps the gateway provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program, including a description of how it has complied with the know-your-upstream provider requirement in § 64.1200(n)(4)”).

DIAL WORLD reviews and, where applicable, updates its STIR/SHAKEN certification selections in the Robocall Mitigation Database in connection with the annual recertification required under 47 C.F.R. § 64.6305(h), and confirms that the certification option selected for each role it performs in the call path (Voice Service Provider, Intermediate Provider, and/or Gateway Provider) accurately reflects DIAL WORLD's current network architecture and STIR/SHAKEN implementation.

II. Robocall Mitigation Program

This RMP applies to DIAL WORLD calling platforms and provides information on DIAL WORLD policies and procedures on the following topics that are discussed in turn below which “details the specific reasonable steps [DIAL WORLD] has taken to avoid carrying or processing illegal robocall traffic”:

- (1) Implementing Knowing Your Customer Protocols
- (2) Implementing Know Your Upstream Provider (KYUP) Protocols
- (3) Requiring Contractual Provisions to Mitigate Illegal Robocalls
- (4) Only Accepting Traffic from Providers in the RMD
- (5) Blocking Calls on a Do-Not-Originate List
- (6) Analyzing and Monitoring Network Traffic Routing Through DIAL WORLD's Network
- (7) Ensuring Foreign Providers Are Not Using DIAL WORLD to Carry or Process High-Volume Illegal Traffic onto the U.S. Network
- (8) Authenticating Voice Traffic Originated by DIAL WORLD
- (9) Responding to Commission, Law Enforcement and ITG Traceback Requests
- (10) Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues
- (11) Training Personnel
- (12) Updating DIAL WORLD's RMD Submission and RMP

1. Implementing Knowing Your Customer Protocols

Consistent with 47 C.F.R. § 64.1200(n)(3) and applicable FCC robocall mitigation requirements, DIAL WORLD takes affirmative and effective measures to prevent new and existing customers from using its network to originate or transmit illegal traffic. DIAL WORLD maintains Know Your Customer (“KYC”) procedures designed to verify the identity and legitimacy of its customers, understand the nature and intended use of the services provided, and assess the risk that its services may be used for illegal robocalling or other unlawful activity.

Prior to onboarding or renewing a customer, DIAL WORLD collects and reviews identifying, corporate, business, and regulatory information. Such information includes, as applicable, the customer’s full legal name, jurisdiction of incorporation, physical and billing addresses, business contact information, nature of business and services provided, website and business email domain, FCC Registration Number (FRN), FCC Form 499 Filer ID, Robocall Mitigation Database (RMD) registration, Operating Company Number (OCN), and STIR/SHAKEN implementation status. DIAL WORLD also evaluates the customer’s role in the call chain, including whether the customer originates calls, acts as an intermediate or gateway provider, or otherwise sends voice traffic to DIAL WORLD.

Where applicable, DIAL WORLD also obtains information regarding the customer’s intended use of DIAL WORLD’s services, expected traffic profile and volumes, countries of origination, and the nature of any originating or telemarketing traffic. DIAL WORLD may request additional information or supporting documentation based on the customer’s business model, traffic profile, regulatory status, or other identified risk factors.

DIAL WORLD validates customer information using available corporate, regulatory, and other reliable sources. Where a customer is required to be registered in the FCC’s RMD, DIAL WORLD confirms that the customer is appropriately listed and has not been de-listed pursuant to an enforcement action before accepting traffic from that provider. DIAL WORLD also reviews relevant regulatory information, including the customer’s RMD certification and Robocall Mitigation Plan, where applicable.

KYC is an ongoing process and is not limited to initial onboarding. DIAL WORLD may periodically review and update customer information and may conduct additional due diligence when there is a material change in the customer’s business, traffic profile, regulatory status, traceback activity, or other circumstances that may indicate increased compliance risk. Failure to provide requested information or otherwise satisfy DIAL WORLD’s KYC and compliance requirements may result in additional monitoring, restriction, suspension, or termination of service.

2. Implementing Know Your Upstream Provider (KYUP) Protocols

Independent of its obligations with respect to foreign-originated traffic described above, DIAL WORLD takes reasonable and effective steps, consistent with 47 C.F.R. § 64.1200(n)(4), with respect to each originating or intermediate provider, whether foreign or domestic, from which it directly receives traffic, to ensure that such provider is not using DIAL WORLD to carry or process illegal traffic.

As part of its Know Your Upstream Provider (“KYUP”) procedures, DIAL WORLD collects and verifies identifying, corporate, and regulatory information regarding its upstream providers, including, as applicable, the provider’s FCC Registration Number (FRN), FCC Form 499 Filer ID, Robocall Mitigation Database (RMD) registration and status, Operating Company Number (OCN), STIR/SHAKEN implementation, and Robocall Mitigation Plan. DIAL WORLD also evaluates the provider’s role in the call chain, the nature and expected profile of the traffic it will send to DIAL WORLD, and whether the provider maintains appropriate Know Your Customer procedures and other measures designed to prevent the origination or transmission of illegal traffic.

DIAL WORLD verifies, as applicable, that upstream providers required to register in the RMD are appropriately listed and have not been de-listed pursuant to an enforcement action. DIAL WORLD also considers available traceback, regulatory, and enforcement information relevant to the provider’s risk profile and monitors traffic received from the provider on an ongoing basis for suspicious or potentially unlawful activity. DIAL WORLD may request additional information or

corrective action and may restrict, suspend, or terminate the exchange of traffic with the provider.

DIAL WORLD maintains records of its KYC and KYUP reviews and validation processes for compliance, auditing, and regulatory purposes.

3. Requiring Contractual Provisions to Mitigate Illegal Robocalls

Voice service customers of DIAL WORLD are subject to robust terms and conditions that (1) obligate customers not to use DIAL WORLD’s services for unlawful purposes; and (2) preserve DIAL WORLD’s right to terminate customers for violations of the law.

DIAL WORLD’s contracts include terms that forbid the customer from using DIAL WORLD’s services to originate and/or otherwise transmit calls that violate laws restricting robocalls or other telemarketing calls, including the federal Telephone Consumer Protection Act (“TCPA”) and/or the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”) and/or the rules promulgated pursuant to these statutes. DIAL WORLD’s contract terms provide that if any calls originated or otherwise transmitted by the customer to DIAL WORLD violate the TCPA, the TRACED Act, or the rules promulgated under these statutes, then DIAL WORLD may, at its sole discretion, suspend or terminate the customer’s service immediately, among other remedies.

4. Only Accepting Traffic from Providers in the RMD

Accepting traffic from domestic Voice Service Providers. In accordance with 47 C.F.R § 64.6305(e)(1), DIAL WORLD accepts calls directly from a domestic Voice Service Provider only if that Voice Service Provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Foreign Voice Service Providers and Foreign Intermediate Providers. In accordance with 47 C.F.R § 64.6305(e)(2), beginning 90 days after the deadline for filing certifications pursuant to 47 C.F.R § 64.6305(d) (which is April 11, 2023), DIAL WORLD accepts calls directly from a Foreign Voice Service Provider or Foreign Intermediate Provider that uses North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States, only if that foreign provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Gateway Providers. In accordance with 47 C.F.R § 64.6305(e)(3), beginning 90 days after the deadline for filing certifications pursuant to 47 C.F.R § 64.6305(d) (which is April 11, 2023), DIAL WORLD accepts calls directly from a Gateway Provider only if that Gateway Provider's filing (a) appears in the RMD showing that the Gateway Provider has affirmatively submitted its filing and RMP, and (b) has not been de-listed pursuant to an enforcement action.

5. Blocking Calls on a Do-Not-Originate List

In accordance with FCC Rules, 47 C.F.R. § 64.1200(k)(2) and (o)(1)-(4), DIAL WORLD blocks calls purporting to originate from a number on a reasonable Do-Not-Originate (“DNO”) list that is associated with North American Numbering Plan numbers. DIAL WORLD has protocols in place to detect DNO calls and blocks calls that are determined to originate from a DNO number. DIAL WORLD is utilizing the DNO list offered by US Telecom. DIAL WORLD does not block calls to 911 and takes reasonable steps to avoid blocking calls originating from public safety answering points (PSAPs) and government emergency numbers.

6. Analyzing and Monitoring Network Traffic Routing Through DIAL WORLD’s Network

DIAL WORLD monitors and analyzes call traffic that originates on, terminates to, or routes through its network to identify suspicious or potentially unlawful traffic. DIAL WORLD monitors traffic patterns and network activity on an ongoing basis, including indicators such as abnormal call volumes or patterns, call duration, excessive call attempts or failures, unusual traffic behavior, and other characteristics that may be associated with illegal robocalling, spoofing, fraud, or other unlawful activity.

DIAL WORLD utilizes third-party switching platforms and analytics tools to support its traffic monitoring, call filtering, fraud prevention, and robocall mitigation activities. DIAL WORLD currently utilizes DeNoVoLab (“DNL”) and Veriswitch as part of its voice traffic and monitoring infrastructure. Through these platforms, DIAL WORLD utilizes YouMail fraud prevention and robocall mitigation features and the Somos Do Not Originate (“DNO”) filter. DIAL WORLD also utilizes Raptor, RoboKiller, Smart Shield AI, and SIP Shield AI as additional tools supporting its traffic monitoring, analytics, filtering, and robocall mitigation efforts.

These third-party platforms and tools operate in conjunction with DIAL WORLD's internal monitoring and compliance procedures to assist in identifying abnormal traffic patterns, suspicious or potentially unlawful traffic, and other indicators requiring further investigation. When potentially problematic traffic is identified, DIAL WORLD investigates the activity and takes appropriate action based on the circumstances, which may include enhanced monitoring, restricting or blocking the affected traffic, requiring corrective action from the responsible customer or provider, suspending service, or terminating the business relationship.

When DIAL WORLD blocks a call based on reasonable analytics designed to identify unwanted or illegal calls, DIAL WORLD uses SIP response code 603+ to provide immediate notification of the blocking determination to the upstream provider, consistent with applicable FCC requirements.

7. Ensuring Foreign Providers Are Not Using DIAL WORLD to Carry or Process High-Volume Illegal Traffic onto the U.S. Network

Pursuant to 47 C.F.R. § 64.1200(n)(4) and its January 16, 2023 effective date, when DIAL WORLD serves as a Gateway Provider for voice traffic that is routing through its network, DIAL WORLD takes reasonable and effective steps discussed under Section 2 and 6, above, to ensure that any Foreign Voice Service Provider or Foreign Intermediate Provider from which DIAL WORLD directly receives traffic is not using DIAL WORLD, as a Gateway Provider, to carry or process a high volume of illegal traffic onto the U.S. network. In addition, as a Gateway Provider, DIAL WORLD blocks – to the best of its ability – foreign originating calls with U.S. North American Numbering Plan numbers in the Caller ID, unless the upstream provider has been previously approved for sending such traffic, based on satisfactory due diligence.

8. Authenticating Voice Traffic

When operating as a Voice Service Provider, DIAL WORLD does the following (1) authenticates and verifies caller identification information for all SIP calls that exclusively transit its own network; (2) authenticates 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 (3) verifies 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 authenticated³.

When operating as an Intermediate Provider, DIAL WORLD passes unaltered, any authenticated caller identification information for all calls it receives that use North

³ 47 C.F.R. § 64.6301(a).

American Numbering Plan resources that pertain to the United States in the caller ID field.

When operating as a Gateway Provider, DIAL WORLD authenticates caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call⁴.

9. Responding to Commission, Law Enforcement and ITG Traceback Requests

DIAL WORLD is committed to ensuring that its network is not utilized for the origination, termination, or routing of illegal robocalls. In accordance with the FCC's regulations, 47 C.F.R. § 64.6305(b)(2) and 47 C.F.R. § 64.1200(n)(1)(ii), DIAL WORLD will respond to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium ("ITG") within 24 hours⁵ and will cooperate with such entities in investigating and stopping illegal robocallers that attempt to use DIAL WORLD's network to carry or process calls. As part of this commitment, DIAL WORLD will take the necessary steps to effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission through its Enforcement Bureau and will comply with the requirements of such notice in accordance with applicable FCC rules⁶.

Upon receipt of a traceback involving traffic associated with a DIAL WORLD customer or upstream provider, DIAL WORLD identifies the relevant customer or upstream provider, preserves the relevant call detail records, responds to the requesting entity within the required timeframe, and investigates the source and nature of the traffic. Based on that investigation, DIAL WORLD takes proportionate action, which may include warning the customer or upstream provider, applying enhanced monitoring, restricting or blocking the traffic, and suspending or terminating service.

10. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues

To further ensure DIAL WORLD's network is not utilized for the origination, termination, or routing of unwanted and illegal robocalls, DIAL WORLD provides the following name, title, department, business address, telephone number, and email address of the individual within DIAL WORLD that leads DIAL WORLD's team that handles robocall mitigation-related issues as well as responds to traceback inquiries from the FCC, ITG, and law enforcement agencies:

⁴ 47 C.F.R. § 64.6302(b) and (c).

⁵ This 24-hour window applies within business days, per rule 47 C.F.R. § 64.1200(n)(1)(ii) and as clarified by the Commission. See FCC 22-37, at n.211.

⁶ See 47 C.F.R. § 64.1200(n)(2), (3) & (5).

Contact Name: Len Bittner

Contact Title: President / Managing Member

Contact City: Wilmington

Contact State and Zip Code: Delaware 19806

Contact Telephone Number: 1+ (855) 800-4562

Contact Email: len@dialworldcom.com

11. Training Personnel

DIAL WORLD provides periodic training to personnel involved in sales, provisioning, network and technical operations, and compliance regarding its robocall-mitigation obligations, including know-your-customer and know-your-upstream-provider procedures, Robocall Mitigation Database verification, STIR/SHAKEN, identification of suspicious traffic, call blocking, and traceback and escalation procedures.

12. Updating DIAL WORLD's RMD Submission and RMP and Annual Recertification

Consistent with 47 C.F.R. § 64.6305, DIAL WORLD will update its submission in the Robocall Mitigation Database ("RMD") within 10 business days of any change to the information required to be provided in the RMD, including any material changes to its Robocall Mitigation Plan. In addition, DIAL WORLD will recertify its RMD filing annually, on or before March 1 of each year, as required by 47 C.F.R. § 64.6305(h). As part of the annual recertification process, DIAL WORLD will review its RMD filing and Robocall Mitigation Plan to ensure that the information remains current, accurate, and complete and will make any necessary updates prior to recertification.