

ROBOCALL MITIGATION PLAN

DIAL UNIVERSAL INC.

1. Company Information

Legal Company Name	Dial Universal Inc.
FCC Registration Number (FRN)	0029447802
FCC Form 499 Filer ID	839115
Type of Service Provider	Voice Service Provider / Intermediate Provider
Effective Date of Plan	07/15/2026
Plan Review Cycle	Reviewed and updated annually, or sooner if regulatory requirements change

2. Purpose and Scope

This Robocall Mitigation Plan (“Plan”) is submitted by Dial Universal Inc. (“the Company”) pursuant to the requirements of the TRACED Act and the rules of the Federal Communications Commission (“FCC”), including 47 C.F.R. § 64.6305. The Plan describes the specific, affirmative, and effective measures the Company has implemented to prevent its network from being used to originate, transmit, or facilitate illegal robocall traffic.

This Plan applies to all voice traffic originated, carried, or terminated by Dial Universal Inc., including traffic exchanged with upstream and downstream providers, and covers all customers provisioned on the Company’s network, whether direct or through reseller arrangements.

3. STIR/SHAKEN Implementation Status

Dial Universal Inc. has fully implemented the STIR/SHAKEN caller ID authentication framework across its network. The Company uses STIR/SHAKEN authentication as an integral part of its robocall mitigation and caller ID authentication program.

The Company has completed the required STIR/SHAKEN implementation and maintains the necessary relationships, credentials, and technical processes to support the authentication of applicable voice calls. Dial Universal Inc. will maintain its STIR/SHAKEN implementation and authentication processes and will continue to monitor and update its deployment as necessary to support ongoing compliance with applicable FCC robocall mitigation and caller ID authentication requirements.

4. Robocall Mitigation Program

Dial Universal Inc. has adopted the following affirmative and effective measures, applied on an ongoing basis, to prevent unlawful use of its network for the origination of illegal robocalls.

4.1 Know Your Customer (KYC) Procedures

- Verification of the legal identity of all customers prior to service activation, including business registration documents, government-issued identification, and tax identification numbers where applicable
- Collection and retention of customer contact information, business use case, and expected call traffic profile
- Risk-based onboarding, under which customers presenting higher-risk profiles (e.g., high-volume outbound calling, telemarketing use cases) are subject to enhanced due diligence
- Ongoing periodic re-verification of existing customers, particularly where traffic patterns materially change

4.2 Traffic Monitoring and Analytics

- Continuous, real-time monitoring of inbound and outbound call traffic across the Company's network
- Use of automated analytics tools to detect calling patterns consistent with illegal robocalling or spoofing, including:
 - Abnormal spikes in call volume from a single customer or number range
 - Abnormally short average call durations
 - High-frequency sequential dialing or auto-dialing patterns
 - Unusually high call-to-completion ratios inconsistent with legitimate traffic
- Escalation of flagged traffic for manual review by compliance staff

4.3 Call Blocking and Filtering

- Immediate suspension or blocking of traffic identified as suspicious, fraudulent, or unlawful
- Deployment of automated fraud-detection and call-filtering systems at the network edge
- Application of analytics-based call blocking consistent with FCC guidance on permissible network-level blocking

4.4 Do-Not-Originate (DNO) Protection

- Blocking of outbound calls that purport to originate from invalid, unallocated, or unassigned numbers
- Blocking of calls spoofing numbers on industry-recognized Do-Not-Originate (DNO) lists (e.g., numbers used by government agencies or financial institutions that do not originate outbound calls)
- Regular updates of internal DNO and number-validation lists in line with industry sources

4.5 Traceback Cooperation

Dial Universal Inc. fully cooperates with traceback requests initiated by industry partners, including the USTelecom Industry Traceback Group (ITG), the FCC, and state attorneys general. The Company:

- Designates a compliance point of contact responsible for responding to traceback requests
- Responds to traceback requests within 24 hours, or within any shorter timeframe required by applicable regulation or the requesting authority
- Takes appropriate mitigation action against any customer identified as a source of illegal robocall traffic through a traceback investigation, up to and including suspension or termination

4.6 Upstream Provider Compliance

- The Company engages only with reputable, compliant upstream carriers that maintain their own robocall mitigation obligations
- Preference is given to upstream providers that have implemented STIR/SHAKEN call authentication
- Upstream provider relationships are periodically reviewed to confirm continued regulatory compliance

4.7 Downstream Customer Enforcement

- Customer service agreements include contractual provisions requiring compliance with the Telephone Consumer Protection Act (TCPA), the Truth in Caller ID Act, and all other applicable robocall and caller ID regulations
- Customers are prohibited from originating illegal robocalls, spoofing caller ID information, or evading network-level call blocking or filtering
- Violations identified through monitoring, complaints, or traceback requests result in a graduated enforcement response, up to and including:
 - Formal warning and required corrective action
 - Immediate suspension of service pending investigation
 - Permanent termination of the customer relationship

4.8 Record Retention

- Call Detail Records (CDRs) are generated and retained for all traffic originated or carried on the Company's network
- Supporting logs, KYC documentation, and traceback correspondence are retained in accordance with FCC recordkeeping requirements
- Records are made available promptly to the FCC, traceback consortia, and other authorized regulatory bodies upon request

4.9 Employee Training and Internal Compliance

- Relevant personnel are trained on robocall mitigation obligations, KYC procedures, and traceback response protocols
- The Company maintains an internal compliance function responsible for overseeing adherence to this Plan

5. Regulatory Compliance and Plan Updates

Dial Universal Inc. complies with all applicable FCC rules and regulations governing robocall mitigation and prevention, including obligations under the Robocall Mitigation Database (RMD) filing requirements. This Plan will be reviewed and updated as necessary to reflect:

- Changes to the Company's STIR/SHAKEN implementation, authentication processes, or related compliance controls
- Updates to applicable FCC rules or industry best practices
- Material changes to the Company's network, customer base, or traffic profile

6. Certification

The undersigned certifies, under penalty of perjury, that the information contained in this Robocall Mitigation Plan is true and accurate to the best of their knowledge, and that Dial Universal Inc. is implementing the robocall mitigation measures described herein.

Signature: Manpreet

Name: Manpreet Goraya

Title: President

Date: 07/15/2026