

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Submitted to the Federal Communications Commission
Robocall Mitigation Database — Pursuant to 47 CFR § 64.6305

Filing Entity:	IORDER SRL LLC
FCC Registration Number (FRN):	0038803292
Business Address:	16192 Coastal Hwy, Lewes, DE 19958, United States
Type of Filing:	Voice Service Provider
STIR/SHAKEN Certification:	Option 3 — No STIR/SHAKEN Implementation (exemption explained in Section III)
Date:	August 20, 2026

I. INTRODUCTION AND PURPOSE

IORDER SRL LLC (“IORDER” or the “Company”) submits this Robocall Mitigation Program Description to the Federal Communications Commission (“Commission” or “FCC”) in connection with its certification in the Robocall Mitigation Database, pursuant to 47 CFR § 64.6305 and the Commission’s filing guidance set forth in Public Notice DA 24-73. This document describes the Company’s role in the call chain, its STIR/SHAKEN caller ID authentication status and the basis for its certification, and the specific, reasonable steps the Company takes to prevent its service from being used to originate illegal robocall traffic.

All calls that IORDER originates on its service are subject to the robocall mitigation program described herein, consistent with 47 CFR § 64.6305(a). The Company commits to participating fully in industry traceback efforts and to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that may attempt to use its service, as set out in Section VII below.

II. COMPANY OVERVIEW AND DESCRIPTION OF SERVICE

IORDER provides a consumer mobile application through which registered users may acquire telephone numbers and use those numbers to place and receive voice calls. The service is designed for ordinary personal and business communications by individual end users. It is not designed for, marketed to, or made available for high-volume outbound calling, autodialing, mass-calling campaigns, or call-center operations, and the Company does not offer bulk origination, dialer integration, or wholesale traffic services of any kind.

IORDER is not a facilities-based carrier. The Company does not own or operate telephone network switching infrastructure, does not interconnect directly with the public switched telephone network, and does not obtain numbering resources directly from the North American Numbering Plan Administrator or the Pooling Administrator. All telephone numbers made available through the application, and all call

origination, transport, and termination, are provided by the Company's underlying U.S.-based carrier platforms: Twilio, Telnyx, and Plivo (together, the "Underlying Carriers"). Every call placed by an IORDER user is originated onto the public telephone network by one of the Underlying Carriers over that carrier's network and subject to that carrier's compliance controls, in addition to the Company's own controls described in this document.

Principals, Affiliates, Subsidiaries, and Parent Companies. Victor Antoci, Director, is the principal of the Company. The Company has no affiliates, subsidiaries, or parent companies.

III. STIR/SHAKEN IMPLEMENTATION STATUS AND BASIS FOR CERTIFICATION

IORDER certifies under Option 3 (No STIR/SHAKEN Implementation) of the Voice Service Provider certification. The Company has not itself implemented the STIR/SHAKEN authentication framework because it lacks control of the network infrastructure necessary to do so and is not presently capable of obtaining a Service Provider Code (SPC) token under the STI Governance Authority's token access policy. The Company relies on the exemption available under 47 CFR § 64.6304(b), which provides that a voice service provider that is incapable of obtaining an SPC token due to Governance Authority policy is exempt from the requirements of 47 CFR § 64.6301 until it is capable of obtaining a token.

This exemption applies to IORDER for the following reasons:

- The Company does not operate its own voice network. It has no softswitch, session border controller, or SIP interconnection with other carriers on which STIR/SHAKEN signing infrastructure could be deployed. All network functions are performed by the Underlying Carriers.
- The Company does not have direct access to numbering resources and does not hold an Operating Company Number (OCN); all telephone numbers used in the service are provisioned through the Underlying Carriers.
- Critically, no call on the IORDER service reaches the public telephone network unauthenticated. Each of the Underlying Carriers — Twilio, Telnyx, and Plivo — has implemented the STIR/SHAKEN framework on its network and signs calls originated on behalf of its customers with its own STI certificates. Calls placed by IORDER users are therefore authenticated at origination by the facilities-based provider that actually places them onto the network.

Should the Company's circumstances change such that it becomes capable of obtaining an SPC token — for example, if it obtains direct access to numbering resources or deploys its own network infrastructure — the Company will register with the STI Policy Administrator, implement STIR/SHAKEN in the IP portions of its network as required by 47 CFR § 64.6301, and update its Robocall Mitigation Database filing accordingly. In the interim, and in all events, all calls originated on the service are subject to the robocall mitigation program described below.

IV. ROBOCALL MITIGATION PROGRAM

The Company's robocall mitigation program consists of the specific, layered measures described in this Section. Taken together, these practices are reasonably designed to prevent the origination of illegal robocall traffic on the IORDER service and to detect and stop any such traffic promptly if it occurs.

A. Know-Your-Customer Procedures (47 CFR § 64.1200(n)(4))

IORDER takes affirmative, effective measures to know its customers and to prevent new and renewing customers from using the service to originate illegal calls:

- **Account registration and identity information.** Every user must create an account before acquiring a number or placing calls. At registration the Company collects and retains identifying information for each customer, including the customer's email address and a mobile telephone number verified by a one-time passcode.
- **Payment verification.** Numbers and calling credit are acquired through paid transactions processed through the Apple App Store and Google Play in-app billing systems, which tie every account to a verifiable payment instrument and further establish customer identity.
- **Carrier-level compliance requirements.** Number provisioning through the Underlying Carriers is subject to those carriers' own regulatory and know-your-customer requirements, which the Company satisfies for the numbers it provisions.
- **Service design limits.** The service is a consumer mobile application in which calls are dialed manually by an individual user from a handset. The application provides no API, no bulk or automated dialing capability, no caller ID spoofing capability (users may present only numbers assigned to their account), and no capability to upload calling lists. These design constraints materially limit the service's usefulness to illegal robocallers.

B. Know-Your-Upstream-Provider Procedures and Contractual Provisions

The Company obtains connectivity exclusively from three established, U.S.-based carrier platforms — Twilio, Telnyx, and Plivo — each of which is registered in the Robocall Mitigation Database, has implemented STIR/SHAKEN, and maintains published acceptable-use and anti-fraud policies. The Company's use of each Underlying Carrier is governed by that carrier's service agreement and acceptable use policy, which contractually prohibit unlawful traffic, including illegal robocalls, and permit suspension of traffic that violates those policies. The Company does not accept or route traffic from any upstream provider other than calls originated by its own registered end users.

IORDER's own Terms of Service, to which every user must agree, expressly prohibit use of the service for unlawful purposes, including the origination of illegal robocalls, automated or prerecorded-voice calling in violation of the Telephone Consumer Protection Act, caller ID spoofing, harassment, and fraud. Violation of these terms is grounds for immediate suspension or termination of the account.

C. Call Analytics and Traffic Monitoring

The Company monitors traffic on its service to identify and stop suspicious calling patterns, using the following systems:

- **Underlying Carrier analytics (third-party systems).** The Company's traffic is screened by the fraud-detection and messaging/voice compliance systems operated by its Underlying Carriers — Twilio, Telnyx, and Plivo — which monitor traffic characteristics across their networks, flag anomalous or abusive calling patterns, and can block or suspend offending traffic. These carrier platforms serve as the Company's third-party analytics vendors.

- **Internal platform monitoring.** The Company reviews per-account usage metrics available through its application backend and the Underlying Carriers' dashboards and alerts, including call volumes, call frequency, and unusual usage patterns inconsistent with ordinary personal calling (for example, sustained high-volume outbound calling or abnormally short call durations). Accounts exhibiting such patterns are investigated and, where warranted, suspended.

D. Complaint Handling and Enforcement

- The Company accepts and reviews complaints regarding misuse of its service, including complaints received directly from users, forwarded by the Underlying Carriers, or received from regulators or law enforcement, at the point of contact identified in Section VIII.
- Upon identifying an account associated with suspected illegal robocall traffic or other unlawful calling, the Company will promptly investigate and take enforcement action, up to and including immediate suspension of calling capability, termination of the account, and reclamation of assigned numbers.
- The Company retains records of customer identifying information, number assignments, and call detail records sufficient to identify the user responsible for any call originated on the service, so that traceback requests can be answered completely and quickly.

V. COMPLIANCE REPRESENTATIONS

- All calls that IORDER originates on its network are subject to the robocall mitigation program described in this document, consistent with 47 CFR § 64.6305(a).
- No prior certification of the Company has been removed from the Robocall Mitigation Database by Commission action, and the Company has not been prohibited from filing in the Robocall Mitigation Database by the Commission.
- The Company has not, at any time in the prior two years, been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the Company transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

VI. COMMITMENT TO TRACEBACK COOPERATION

IORDER commits to respond fully, and within 24 hours, to all traceback requests received from the Commission, law enforcement, and the industry traceback consortium (currently the Industry Traceback Group). The Company's designated robocall mitigation point of contact (Section VIII) is responsible for receiving such requests and for providing complete responses, including identification of the customer account, the customer identifying information on file, and relevant call detail records.

VII. COMMITMENT TO COOPERATE IN INVESTIGATING AND STOPPING ILLEGAL ROBOCALLERS

The Company commits to cooperate with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that use its service to originate calls. This

includes timely production of records, suspension or termination of offending accounts upon identification, and implementation of any additional mitigation measures reasonably necessary to prevent recurrence.

VIII. ROBOCALL MITIGATION POINT OF CONTACT

Name: Victor Antoci
Title: Director
Company: IORDER SRL LLC
Address: 16192 Coastal Hwy, Lewes, DE 19958, United States
Telephone: +1 513 743 3113
Email: office@multicallapp.com

IX. CONCLUSION

The measures described above constitute IORDER's robocall mitigation program. The Company believes these practices, in combination with the STIR/SHAKEN authentication performed by its Underlying Carriers, can reasonably be expected to significantly reduce the risk of illegal robocalls originating on its service. The Company will keep this program description current and will update its Robocall Mitigation Database filing within the timeframes required by the Commission's rules whenever the information in this filing changes, and will recertify annually as required.

Respectfully submitted,

Victor Antoci

Date: 08.20.2026

Victor Antoci, Director

IORDER SRL LLC — FRN 0038803292