

NOHL INC

Robocall Mitigation Program Description

Prepared for filing in the FCC Robocall Mitigation Database October 21, 2026

1. Introduction and Role in the Call Path

Nohl Inc. ("Nohl") operates a software platform that provides voice calling and related business-communication tools to business customers. Nohl is a voice service provider for purposes of this filing.

Nohl does not own or operate a telephone network, does not hold telephone numbers directly, and does not interconnect with other carriers. All voice traffic originated by Nohl's customers is carried by Telnyx LLC ("Telnyx"), Nohl's upstream carrier, through managed carrier accounts provisioned under Nohl for each customer. Telephone numbers used on the platform are provisioned through Telnyx under the customer's managed account. Customers may not bring their own telephone numbers, carrier accounts, or carrier credentials to the platform, and may originate calls only from numbers provisioned to their own verified account.

This document describes Nohl's robocall mitigation program, adopted pursuant to 47 CFR § 64.6305, and the specific reasonable steps Nohl has taken to avoid originating illegal robocall traffic. The program applies to all voice traffic originated through the Nohl platform.

2. STIR/SHAKEN Caller ID Authentication

Nohl maintains no STIR/SHAKEN implementation of its own, because it operates no network facilities on which calls originate. All calls originated through the Nohl platform are transmitted by Telnyx, which has fully implemented the STIR/SHAKEN authentication framework, and all such calls are authenticated and signed consistent with 47 CFR § 64.6301. Nohl's certification in this filing is accordingly that it has no STIR/SHAKEN implementation of its own: one hundred percent of the voice traffic originated through Nohl is carried and signed on Telnyx's fully implemented network, and no portion of that traffic is transmitted unsigned.

3. Customer Vetting Before Origination

No customer may obtain telephone numbers or originate calls through the platform until its identity has been verified. Nohl's onboarding requires business identity verification (KYB) and identity verification of the responsible individual (KYC), performed through Stripe Identity. The platform's number-purchase and calling functions are gated on the verified identity record: an account whose verification has not passed cannot obtain numbers and cannot place outbound calls.

Verification status is read from the verification record at the time of purchase and at the time of origination; it is not self-declared by the customer.

4. Customer Obligations: Consent, Do-Not-Call, and Records

Before a customer's first outbound calling campaign, an authorized representative of the customer must complete a recorded attestation. The attestation is retained by Nohl as an append-only record identifying the customer, the attesting user, the timestamp, and the attestation version, and a customer that has not completed it cannot place outbound calls. In the attestation, the customer attests that: (1) the numbers it calls through Nohl are people who consented to be contacted by the customer, the customer's own customers, or people with an established business relationship with the customer; (2) for any number without that basis, the customer checks the National Do-Not-Call Registry and the state do-not-call lists that apply to its calling at least every 31 days, and keeps records of those checks and of the consent or relationship behind the numbers it calls, kept for at least four years and available upon request; (3) anyone who asks the customer not to call is put on the customer's do-not-call list and is not called again; and (4) the customer is responsible for complying with the TCPA, the Telemarketing Sales Rule, and state calling laws for the calls it places. Nohl provides its customers a Do-Not-Call check at contact import, performed using the customer's own DNC service credentials, and communicates these obligations to customers during onboarding and in the platform. Responsibility for the lawfulness of a customer's campaigns rests with the customer; Nohl's role is to require the attestation, provide the tooling described in Section 5, and enforce as described in Section 6.

5. Ongoing Controls and Monitoring

Suppression enforcement. The platform maintains account-level suppression lists. A customer can record a do-not-contact request against a number, and any number on an account's suppression list is blocked server-side at the moment of dialing, on every outbound dial path, before the call is placed. Opt-outs received through the platform — including inbound text-message STOP requests — are recorded as suppressions and honored immediately.

Calling windows. Each outbound dial is evaluated against recipient-local calling hours (8:00 a.m. to 8:00 p.m. recipient local time, with stricter state rules applied where they govern) at the time of the dial; calls outside the window are refused.

Origination limits. The platform enforces rate limits on outbound call origination, applied per account and per number. Nohl's operations personnel can set account-level call volume and spending limits.

Records and review. The platform maintains per-account call detail records. Nohl's operations personnel review account calling activity, respond to reports of unlawful traffic, and escalate suspected illegal robocall activity to the robocall mitigation contact named in Section 8.

6. Enforcement

A customer found to be originating illegal robocall traffic, or to be failing to maintain the consent records required by Section 4, is subject to immediate suspension of origination privileges pending investigation and to termination of service. Nohl can disable a customer's outbound calling immediately at the platform level, and maintains a platform-level control capable of halting all outbound calling. Nohl cooperates with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that use its service.

7. Traceback Commitment

Nohl will respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Group, and will cooperate with such entities, and with other voice service providers, in investigating and stopping the source of any illegal robocall traffic.

8. Robocall Mitigation Contact

Questions regarding this program may be directed to Nohl's robocall mitigation point of contact:

Aiden Alvarez Chief Executive Officer Nohl Inc.

Updates

Nohl will update this description, and its Robocall Mitigation Database filing, within ten business days of any material change to the program described above, as required by 47 CFR § 64.6305.