

## Purpose

This memo explains the MODX intake and routing controls used when third-party marketers ("POA") distribute MODX entry materials. The design ensures third parties do not perform investor qualification, do not provide advice, and do not control dashboard access.

## System Overview

MODX uses a two-layer intake structure:

- Level 0: Entry & Interest Declaration (informational routing only; no sensitive verification).
- Level 1: Role-specific onboarding (verification, permissioning, and activation) hosted and controlled exclusively by MODX.

## Third-Party Separation (POA)

POA partners are restricted to distributing Level 0 materials or MODX-provided links. POA partners:

- do not modify or host Level 1 forms;
- do not approve or reject applicants;
- do not provide investment advice or qualification decisions;
- do not receive credentialed access to MODX dashboards.

## Routing & Access Controls

Level 0 captures intent and self-identified role. Based on selection, users are routed to:

- Retail preview flows, or
- Level 1 onboarding pages (MODX-only).

Dashboard access is gated by Level 1 completion and MODX-controlled policy checks (jurisdiction, required disclosures, and identity verification as applicable).

## Data Governance

All intake submissions and metadata are stored in MODX-controlled systems. POA tracking parameters may be captured for attribution, but attribution does not grant POA any decision authority or data custody.

## Auditability / Tamper Evidence

Each submission can be recorded with an immutable audit record that includes:

- intake\_id (UUID), timestamp (ISO-8601),
- form\_version, source, tracking parameters,
- SHA-256 hash of the normalized payload plus timestamp and server-side salt.

This provides integrity verification for compliance review and internal controls.

## No Offer / No Solicitation Statement

Level 0 forms and landing pages include clear statements that submissions are informational only and do not constitute an offer, solicitation, approval, or commitment.

## Conclusion

The intake architecture is designed to (1) preserve MODX control over onboarding and access, (2) restrict third parties to distribution-only functions, and (3) maintain auditable records suitable for compliance review.