THINKING OS™

SEAL External Proof Packet

Unauthorized Filing Refusal at the Final Submit Boundary
Evaluator-visible proof of a real pre-execution governance control

Public • Redacted • v1.1 • April 2026

Doc ID: TOS-SEAL-EPP-v1.1-7j5k6l

Document: SEAL External Proof Packet
Version: v1.1 (Public • Redacted) – April 2026
Owner: Thinking OS™
Use: May be shared externally. For information only; not legal advice.

This packet is designed to let legal, risk, insurer, regulator-facing, and technical evaluators assess one narrow claim:

SEAL is a pre-execution authority gate that sits in front of the final filing step and returns approve, refuse, or supervised outcomes before a motion or submission leaves the firm.

For each governed outcome, SEAL produces a reviewable decision artifact. This packet shows evaluator-visible behavior and evidence surfaces for that workflow. It does not expose non-public runtime details.

What This Packet Is For

This is not a product brochure, architecture guide, or diligence binder. It is a proof packet for one governed workflow:

wrong-authority filing refusal at the final submit boundary.

Its purpose is to let a serious buyer or evaluator determine, from the outside, whether:

- the runtime is real
- refusal behavior is real
- decision artifacts are real
- the downstream gate behavior is demonstrable for the scoped workflow under the configured evaluator conditions
- SEAL is a runtime control, not a chat wrapper, dashboard, or policy slideshow

What You Can Verify In 3 Minutes

Inside this packet, you will see:

- why the Commit Layer exists for high-risk legal actions
- where SEAL sits in a wired legal workflow
- one real approval artifact
- three real refusal artifacts from different families
- one supervised / override outcome
- one execution receipt set showing runtime behavior and artifact linkage
- one scoped non-bypassability proof page
- one page on who owns the rules, the runtime, and the proof
- one page on what SEAL does not do

Disclaimer: For information only. Not legal advice. This packet is a public evaluation reference for one narrow governed workflow.

Proof Provenance & Evaluation Boundary

This packet is a public, redacted proof packet for one scoped SEAL Legal Runtime workflow:

Unauthorized / wrong-authority filing refusal at the final-submit boundary.

It is designed to show evaluator-visible runtime behavior, governed outcomes, decision artifacts, execution receipt linkage, and scoped non-bypassability evidence for that workflow. It does not expose non-public runtime internals, secrets, customer data, or production infrastructure details.

Evidence Source

The exhibits in this packet are redacted outputs from a Thinking OS™ internal / evaluator-controlled runtime environment configured to demonstrate the scoped workflow.

The packet may include:

- governed request examples
- approve, refuse, and supervised / override outcomes
- sealed decision artifacts
- audit trace references
- policy and rule-basis references
- integrity / review references
- execution receipt examples
- downstream handling or rejection evidence where shown

What This Packet Shows

For the scoped workflow and configured test conditions, this packet shows that SEAL can:

- receive a structured governed-action request before the final-submit boundary
- evaluate the request against configured role, authority, consent, workflow, and policy conditions
- return approve, refuse, or supervised outcomes
- produce reviewable decision artifacts
- preserve linkage between request, decision, artifact, and execution / handling evidence where configured
- reject direct downstream attempts where the demo workflow requires a valid governed path

What This Packet Does Not Show

This packet does not prove:

- customer-specific deployment readiness
- correctness of any specific law firm's policy
- correctness of any jurisdiction-specific legal rule
- production non-bypassability inside a buyer's environment
- that SEAL replaces lawyer judgment, court rules, GRC, identity systems, DMS, filing tools, or matter systems
- that any buyer has deployed SEAL in production

Redactions and Exclusions

The public packet redacts or excludes:

- runtime internals
- secrets and credentials
- tenant-sensitive identifiers
- operational contact details
- live internal destinations
- security-sensitive configuration
- non-public policy internals
- customer or prospect information

Evaluation Note

This packet should be evaluated as proof of scoped runtime behavior, not as a representation of a completed customer production deployment.

A production or enforcement deployment requires separate client-specific scoping, authority mapping, integration review, security review, and written agreement.

For information only. Not legal advice.

Table of Contents:

Why This Layer Exists **9**
Where SEAL Sits in the Legal Stack **11**
Proof of Approval Under Governed Conditions **13**
How to Read This Approval Artifact 15
Key Verification Points 15
Proof of Refusal Before Harm **16**
Scenario 16
What SEAL returned 16
Why it matters 16
Caption 16
Refusal A — Wrong authority / role not authorized 17
Scenario 19
What SEAL returned 19
Why it matters 19
Bottom line 19
Refusal B — Role disallowed / structurally barred actor 20
Scenario 22
What SEAL returned 22
Why it matters 22
Caption 22
Refusal C — Missing consent / authority condition not satisfied 23
Scenario 25
What SEAL returned 25
Why it matters 25
Caption 25
Proof of Supervised Escalation **26**
Scenario 30
What SEAL returned 30
Why it matters 30
Execution Receipts and Artifacts Tell the Same Story **31**
Block 1 — Governed request received 31
Block 2 — Decision returned 31

Block 3 — Artifact emitted..... 32
Block 4 — Downstream handling event..... 32
Scoped Non-Bypassability for the Demo Workflow..... 33
Block 1 — Approved path through SEAL..... 33
Block 2 — Direct call attempt to commit target..... 34
Block 3 — Deterministic rejection on repeat..... 34
Bottom takeaway..... 34
Who Owns the Rules, the Runtime, and the Proof..... 35
The firm owns..... 35
Thinking OS is responsible for..... 35
What This Runtime Is Not..... 36

Why This Layer Exists

Most institutional and AI governance stops too soon.

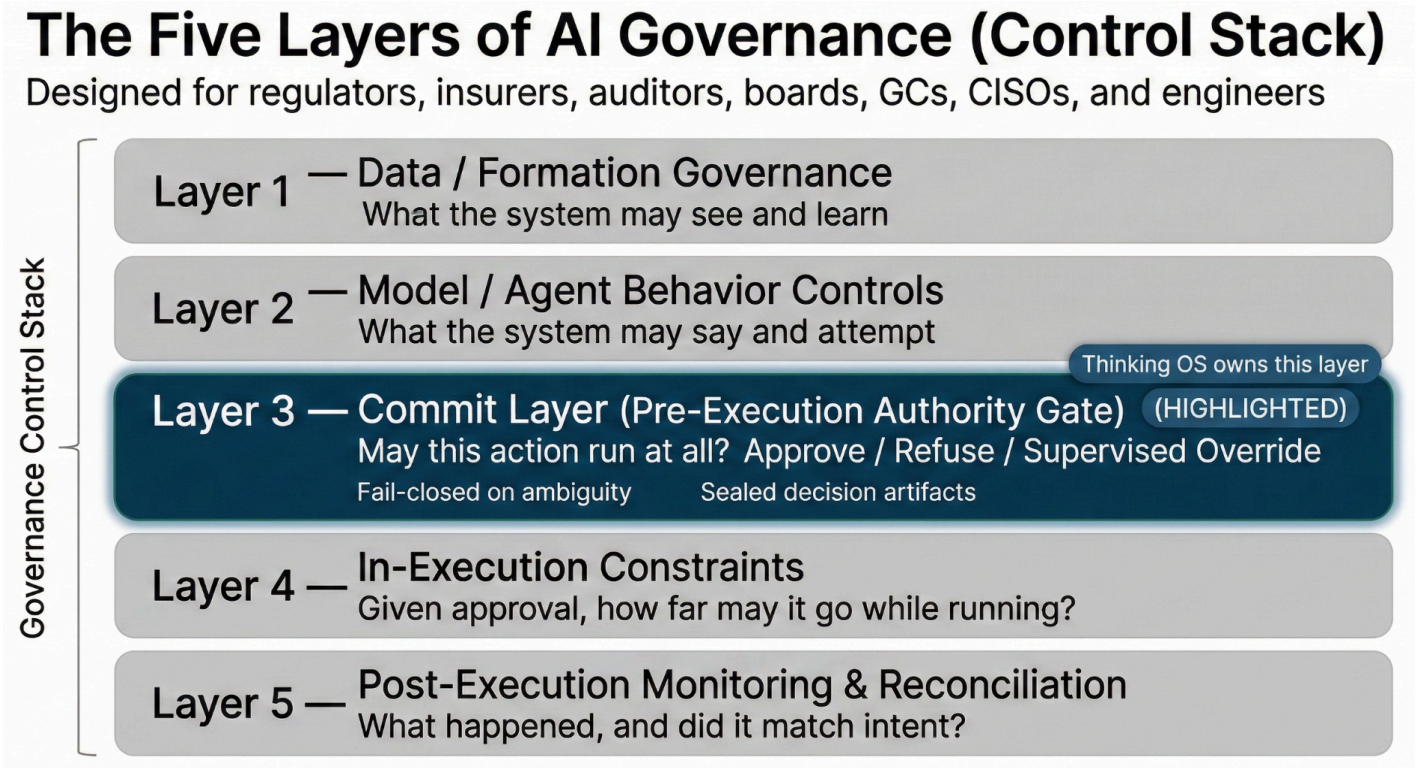
Organizations built data governance, model governance, and identity and access controls first. All of those layers matter. But they do not answer the one question that matters most at the moment of action:

For this actor, this action, right now — may it run at all?

That question belongs to the **Commit Layer**: the pre-execution authority gate in front of high-risk actions.

In legal workflows, that distinction matters because liability attaches when something is filed, sent, approved, or moved under the firm's name — not when a policy is written, a dashboard is reviewed, or a model is monitored later.

SEAL operates at that missing layer for governed legal workflows.



Most governance layers govern what a system may see, say, or how it is reviewed later. **SEAL operates at the missing Commit Layer:** the pre-execution authority gate in front of file / send / approve / move. It returns approve, refuse, or supervised outcomes before the action executes.

This is why SEAL is not ordinary guardrails or after-the-fact monitoring. It governs the moment before the action becomes real.

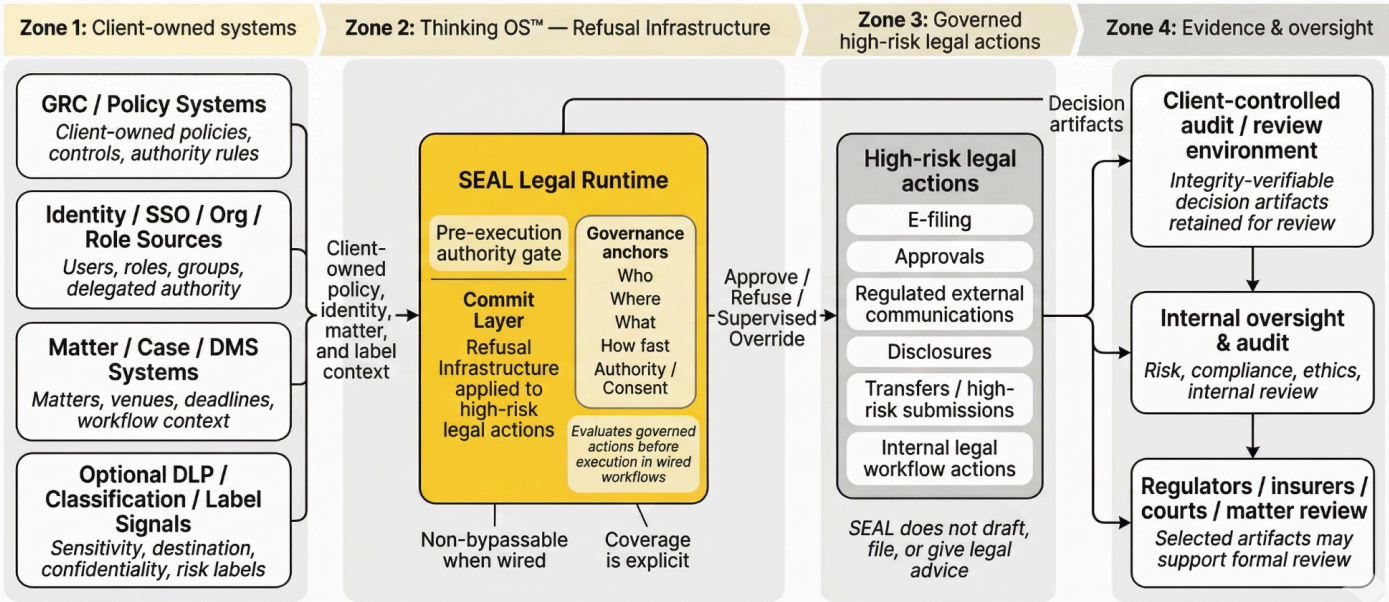
Where SEAL Sits in the Legal Stack

SEAL is not another application for lawyers to log into. It is an upstream control layer that sits between the firm's own policy, identity, matter systems and designated high-risk legal actions.

In a wired workflow, firm-owned systems provide the policy, identity, matter, and label context. SEAL evaluates that governed request at the Commit Layer and returns one of three outcomes: approve, refuse, or supervised override. Downstream tools and workflows proceed only from that governed outcome, and decision artifacts are produced for audit, oversight, and later review where appropriate.

This is the point of control in the workflow: not after the filing, not in a dashboard, and not as a policy reminder after the fact.

Figure 1 — Public Control Map: Where SEAL Sits in the Legal Stack
Action Governance at the Commit Layer for High-Risk Legal Actions



Conceptual control map for public evaluation. Describes evaluator-visible behavior and evidence surfaces, not non-public runtime details.

SEAL sits between firm-owned policy, identity, matter sources and designated high-risk legal actions. Your systems feed SEAL; your drafting and e-filing tools run only once SEAL has approved; and courts, regulators, insurers, and internal oversight functions can review the resulting decision artifacts where appropriate.

This page shows that SEAL is a control point in the workflow, not a dashboard or sidecar.

Proof of Approval Under Governed Conditions

This exhibit shows a governed approval returned by SEAL for the narrow workflow in scope: a final filing request evaluated under the firm's configured authority, consent, and policy conditions. The request was submitted through the strict runtime path for `administrative_law / motion_to_extend_time`, with an attorney actor, valid authority and evidence tokens, consent present, and sufficient time to deadline. The runtime returned an approval outcome and produced a sealed approval artifact with its own trace and integrity references.

Thinking OS™ – SEAL Enforcement Artifact
Case ID: [redacted]
Artifact ID: [redacted]
Timestamp (UTC): 2026-04-07T16:58:18.318225Z

Status: Approval record generated; see runtime outcome below.
Reason: Approved. Identity verified [redacted]. Scope validated: administrative_law • motion_to_extend_time per policy SEAL-APP-ALLOWED-001. Authority/evidence posture: authority=inline_authority (required); evidence=inline_evidence (required).
Next step: Follow your firm's implementation and record-keeping procedures; see detailed reasoning below.
Risk class: Not Classified
Enforcement: Enforce (runtime decisions are applied in-line with governance policy).
Governance decided: approval
Runtime decided: approval
Decision alignment: aligned
Control meaning: Governance approved and required downstream execution completed successfully.

Declared Role	Attorney
Declared Vertical	Administrative Law
Declared Scenario	Motion to Extend Time
Case Stage	Filing
Legal Environment	Administrative Law
Requested Turnaround	Standard
Case Notes (verbatim input; redacted per policy)	[suppressed by policy]
Approval Code	SEAL-APP-ALLOWED-001
Reviewer	[redacted]
Client ID	CLIENT-DEMO-MIDLAW-STRICT
Audit Trace ID	1967e9fd-e9d4-4671-87d2-d5503831d52b
Contact Advisory	[redacted]
Advisory Action Link	[redacted]
Governance Reference	Governance Reference Sheet
Policy Mode (Client Regimen)	Client GRC Regime
Client Environment	Prod
Enforcement Posture	Enforce (runtime decisions are applied in-line with governance policy).
Policy Version	v1.0
Jurisdiction	US-VA

Rule Basis & Authority

Rule-Basis Evidence

- Evidence Decision ID: `9ad862df41d44a158b912d8646f62497`
- Policy Reference: `CLIENT-DEMO-MIDLAW-STRICT:mock-prod/administrative_law/motion_to_extend_time@v1.0`
- Consent requirement: SEAL-CONSENT-001 for administrative_law/motion_to_extend_time.
- Scope: administrative_law/motion_to_extend_time.
- Reviewer role: attorney (claims-mapped from groups).

Artifact HTML Hash: `sha256:24ba5302fc5c3c5170f070b14ecf485593e08b423e91bc28d4cbbb96eed18629` (sha256 over artifact contents above).
Approval Origin: SEAL Runtime Governance Layer.
Governance Approval Hash: `b8aee30b1c69bbcb0a6974d4c2d01250cf243079e0d9da3b5fb72e6ecfa1be31`.
Issued By: Thinking OS™ — Enforcement Core (SEAL-Mode Enabled).
Chain of Custody: Approval chain locked at runtime. Immutable and audit-ready. Field values not declared by input were substituted with explicit runtime fallbacks.
Audit Echo: Metadata logged for oversight and verification only.
Artifact Link: Open sealed artifact
Oversight Registry Reference: Firm Oversight Registry [redacted]
External Compliance Mapping: Firm Standards Map [redacted])
Policy Fingerprint: `sha256:94817e2b03507e9eabd6498d7a492e2ae5761a6c4a675e072da7773ed429db4b`.
Runtime Config Snapshot: `sha256:84a6dd5c5c04b8be3a416b2d8ae901049b69f3be586965a78b4ee6bca6264fb6`.

Redacted public exhibit. Reviewer identity, matter-routing details, operational contact details, and live internal link destinations removed. Decision, policy, trace, and integrity references preserved.

How to Read This Approval Artifact

When SEAL approves a governed filing, it produces a sealed approval artifact showing that the request met the firm's configured governance conditions at the time of action. This exhibit preserves the decision outcome, governance anchors, policy reference, trace reference, and integrity surfaces needed for later review. SEAL approval is a governance pre-condition, not a substitute for legal judgment. Public materials already state that approvals produce audit-ready artifacts and do not replace legal judgment.

Key Verification Points

1. **Decision / Trace Reference** — unique record used to correlate the governed decision later.
2. **Governance Anchors in Force** — role, environment, filing type, stage, turnaround, and related decision context evaluated at decision time.
3. **Approval Outcome** — governed approval returned under the firm's configured rules.
4. **Rule / Policy Reference** — client-owned policy reference applied to this request.
5. **Integrity / Review Reference** — artifact and approval hashes, origin, and chain-of-custody references preserved for audit and later review.

Proof of Refusal Before Harm

Scenario

A filing request was submitted for `administrative_law / motion_to_extend_time` under the strict runtime path. The motion, timing, and consent posture were otherwise valid, but the acting role did not resolve to an authorized legal role from trusted identity claims.

What SEAL returned

SEAL returned a sealed refusal before the filing left the firm. The artifact preserved the refusal code family, audit trace reference, policy reference, and refusal integrity hash.

Why it matters

This is the wedge in concrete form: wrong actor, wrong authority, blocked before external exposure. It shows that SEAL does not merely warn or annotate. It refuses the action at the governed boundary. Public materials explicitly state that unknown or unmapped roles are refused and that fail-closed ambiguity results in sealed refusals, not silent passes.

Caption

This exhibit shows a governed refusal produced before the filing left the firm. The artifact records who attempted the action, what was attempted, which policy context applied, and why the action was blocked. Public materials describe refusals as structured alerts tied to the firm's own rules and inputs, not post-hoc opinions.

Refusal A — Wrong authority / role not authorized

Thinking OS™ – SEAL Enforcement Artifact
Case ID: 74b35bf2-b9c4-460e-850a-a2ebda9b6a40
Artifact ID: 20260409211057-d13226
Timestamp (UTC): 2026-04-09T21:10:53.730537Z

Status: Refusal record generated; see governance and runtime outcome below.
Reason: Code-family explanation applied (display-only); Policy reference: SEAL-ROLE-NOT-AUTHORIZED; This explainer describes how SEAL applied firm-owned configuration to this request; it is not legal advice or a merits opinion.; Designed to support alignment with ABA Model Rule 5.5 (unauthorized practice of law).; Designed to support alignment with ISO 37301 (compliance management systems).; Designed to support alignment with FRCP Rule 11 (frivolous filings prohibition).; Role 'general_counsel' is not in authorized_roles for vertical 'administrative_law'; Governance requires an explicitly authorized legal role for this vertical
Next step: No next-step instructions were provided to SEAL. Refer to your firm's escalation and filing procedures; SEAL does not prescribe remediation or timeframes.
Risk class: Not Classified
Enforcement: Enforce (runtime refusals are applied in-line with governance policy).

Unless otherwise noted, the fields in the table below were declared by the firm's own systems (IdP, matter/case systems, GRC). Entries shown as "Not Declared" indicate that no value was provided to SEAL at runtime; the runtime did not infer or alter those values.

Declared Role	General Counsel
Declared Vertical	Administrative Law
Declared Scenario	Motion To Extend Time
Case Stage	Filing
Legal Environment	Administrative Law
Requested Turnaround	Standard
Refusal Code	SEAL-ROLE-NOT-AUTHORIZED
Severity	Block
Reviewer	[redacted]
Client ID	CLIENT-DEMO-MIDLAW-STRICT
Audit Trace ID	afbb02eb-ebf7-4190-9227-7ef06b306415
Contact Advisory	Governance & Compliance / [redacted]
Advisory Action Link	[redacted]
Governance Reference	[redacted]
Auto-Reroute Triggered	No
Policy Mode (Client Regimen)	Client GRC Regime
Client Environment	Prod
Enforcement Posture	Enforce (runtime refusals are applied in-line with governance policy).
Policy Version	v1.0
Jurisdiction	US-VA

Governance Outcome Record

Outcome: Refusal

This section records the outcome and supporting inputs produced by the governance engine enforcing firm-owned policies. It is not legal advice or a legal opinion.

Summary (verbatim inputs): Code-family explanation applied (display-only); Policy reference: SEAL-ROLE-NOT-AUTHORIZED; This explainer describes how SEAL applied firm-owned configuration to this request; it is not legal advice or a merits opinion.; Designed to support alignment with ABA Model Rule 5.5 (unauthorized practice of law).; Designed to support alignment with ISO 37301 (compliance management systems).; Designed to support alignment with FRCP Rule 11 (frivolous filings prohibition).; Role 'general_counsel' is not in authorized_roles for vertical 'administrative_law'; Governance requires an explicitly authorized legal role for this vertical

Procedural Defects

- Code-family explanation applied (display-only)

Oversight Advisory

- Filing blocked under SEAL governance protocol; oversight review logged.

Rule Basis

- Policy reference: SEAL-ROLE-NOT-AUTHORIZED
- This explainer describes how SEAL applied firm-owned configuration to this request; it is not legal advice or a merits opinion.
- Designed to support alignment with ABA Model Rule 5.5 (unauthorized practice of law).
- Designed to support alignment with ISO 37301 (compliance management systems).
- Designed to support alignment with FRCP Rule 11 (frivolous filings prohibition).

Rule-Basis Evidence & Authority

Rule-Basis Evidence

- Evidence Decision ID: `26d2657b6d5e4d408e36a05a3a1824d0`
- Policy Reference: `CLIENT-DEMO-MIDLAW-STRICT:mock-prod/administrative_law/motion_to_extend_time@v1.0`
- Consent requirement: SEAL-CONSENT-001 for administrative_law/motion_to_extend_time.
- Scope: administrative_law/motion_to_extend_time.
- Reviewer role derived from trusted claims/groups.

Governance Summary (Short Form)

- Role 'general_counsel' is not in authorized_roles for vertical 'administrative_law'
- Governance requires an explicitly authorized legal role for this vertical

External Standards & Firm Mapping

This section is provided for regulators, insurers, and oversight functions that need to see how this refusal maps to the firm's external standards registry and compliance library.

Oversight Registry Reference: [redacted]
External Compliance Mapping: [redacted]

Artifact HTML Hash: sha256:199d9c93683ed78f256c7a752ca9da0731b64a837ba262871c6e819940caa22a (sha256 over artifact contents above)
Governance Refusal Hash: sha256:738057830a1951aeddaf50570b7167703016f7d4edd278677649001222280c35
Refusal Origin: SEAL Runtime Governance Layer
Issued By: Thinking OS™ — Enforcement Core (SEAL-Mode Enabled)
Chain of Custody: Refusal chain locked at runtime. Immutable and audit-ready. Field values not declared by input were substituted with explicit runtime fallbacks.
🔍 **Audit Echo:** Metadata logged for oversight and verification only.
Artifact Link: [redacted]

Scenario

A governed filing request was submitted under the strict runtime path for **Administrative Law / Motion To Extend Time**. The acting role resolved to **General Counsel**, but that role was not configured as an authorized filing role for this governed motion under the tenant's policy.

What SEAL returned

SEAL returned a sealed refusal with code **SEAL-ROLE-NOT-AUTHORIZED**, plus an audit trace reference, policy reference, rule-basis evidence, and refusal integrity surfaces.

Why it matters

This shows that SEAL enforces workflow-specific authority, not job-title prestige. Even a senior legal role is blocked when it is outside the firm's configured authorization scope for the action at issue.

Bottom line

SEAL does not care that the actor is senior. It cares whether the actor is authorized for this governed action under this tenant's rules.

Redacted public exhibit. Reviewer identity, matter-routing details, operational contact details, and live internal link destinations removed. Decision, policy, trace, and integrity references preserved.

Refusal B — Role disallowed / structurally barred actor

Thinking OS™ – SEAL Enforcement Artifact
Case ID: 2bda3126-73a3-421e-8be9-e3175a80b3ba
Artifact ID: 20260408235530-c99733
Timestamp (UTC): 2026-04-08T23:55:26.608750Z

Status: Refusal record generated; see governance and runtime outcome below.
Reason: Code-family explanation applied (display-only); Policy reference: SEAL-ROLE-DISALLOWED; This explainer describes how SEAL applied firm-owned configuration to this request; it is not legal advice or a merits opinion.; Designed to support alignment with ABA Model Rule 5.5 (unauthorized practice of law).; Designed to support alignment with ISO 37301 (compliance management systems).; Designed to support alignment with FRCP Rule 11 (frivolous filings prohibition).; Role 'paralegal' is explicitly disallowed under the administrative_law vertical policy; Governance defaults to fail-closed for unlicensed or disallowed roles
Next step: No next-step instructions were provided to SEAL. Refer to your firm's escalation and filing procedures; SEAL does not prescribe remediation or timeframes.
Risk class: Not Classified
Enforcement: Enforce (runtime refusals are applied in-line with governance policy).

Unless otherwise noted, the fields in the table below were declared by the firm's own systems (IdP, matter/case systems, GRC). Entries shown as "Not Declared" indicate that no value was provided to SEAL at runtime; the runtime did not infer or alter those values.

Declared Role	Paralegal
Declared Vertical	Administrative Law
Declared Scenario	Motion To Compel Production
Case Stage	Administrative Discovery
Legal Environment	Administrative Law
Requested Turnaround	Standard
Refusal Code	SEAL-ROLE-DISALLOWED
Severity	Block
Reviewer	[redacted]
Client ID	CLIENT-DEMO-MIDLAW-STRICT
Audit Trace ID	4526162e-1c9b-4fe2-83d8-851f3efa6381
Contact Advisory	Governance & Compliance [redacted]
Advisory Action Link	[redacted]
Governance Reference	[redacted]
Auto-Reroute Triggered	No
Policy Mode (Client Regimen)	Client GRC Regime
Client Environment	Prod
Enforcement Posture	Enforce (runtime refusals are applied in-line with governance policy).
Policy Version	v1.0

Governance Outcome Record

Outcome: Refusal

This section records the outcome and supporting inputs produced by the governance engine enforcing firm-owned policies. It is not legal advice or a legal opinion.

Summary (verbatim inputs): Code-family explanation applied (display-only); Policy reference: SEAL-ROLE-DISALLOWED; This explainer describes how SEAL applied firm-owned configuration to this request; it is not legal advice or a merits opinion.; Designed to support alignment with ABA Model Rule 5.5 (unauthorized practice of law).; Designed to support alignment with ISO 37301 (compliance management systems).; Designed to support alignment with FRCP Rule 11 (frivolous filings prohibition).; Role 'paralegal' is explicitly disallowed under the administrative_law vertical policy; Governance defaults to fail-closed for unlicensed or disallowed roles

Rule Basis

- Policy reference: SEAL-ROLE-DISALLOWED
- This explainer describes how SEAL applied firm-owned configuration to this request; it is not legal advice or a merits opinion.
- Designed to support alignment with ABA Model Rule 5.5 (unauthorized practice of law).
- Designed to support alignment with ISO 37301 (compliance management systems).
- Designed to support alignment with FRCP Rule 11 (frivolous filings prohibition).

Rule-Basis Evidence & Authority

Rule-Basis Evidence

- Evidence Decision ID: `a168843908934858b2e82aef1874f1cf`
- Policy Reference: `CLIENT-DEMO-MIDLAW-STRICT:mock-prod/administrative_law/motion_to_compel_production@v1.0`
- Consent requirement: SEAL-CONSENT-001 for administrative_law/motion_to_compel_production.
- Scope: administrative_law/motion_to_compel_production.
- Reviewer role derived from claims/group mapping.

Governance Summary (Short Form)

- Role 'paralegal' is explicitly disallowed under the administrative_law vertical policy
- Governance defaults to fail-closed for unlicensed or disallowed roles

External Standards & Firm Mapping

This section is provided for regulators, insurers, and oversight functions that need to see how this refusal maps to the firm's external standards registry and compliance library.

Oversight Registry Reference: [redacted]
External Compliance Mapping: [redacted]

Artifact HTML Hash: sha256:7461f3cf5a4774e93784755975b31bbc66ea981417eea0570c54703caef075eb (sha256 over artifact contents above)
Governance Refusal Hash: sha256:f0fb6e1a97eaeef3ef158ab395c5a782255374ed65fc2ca6ea65338f2ce7b9fd
Refusal Origin: SEAL Runtime Governance Layer
Issued By: Thinking OS™ — Enforcement Core (SEAL-Mode Enabled)
Chain of Custody: Refusal chain locked at runtime. Immutable and audit-ready. Field values not declared by input were substituted with explicit runtime fallbacks.
🔍 **Audit Echo:** Metadata logged for oversight and verification only.
Artifact Link: [redacted]

Scenario

A governed legal action was submitted under the strict runtime path for **Administrative Law / Motion To Compel Production**. The acting role resolved to **paralegal** from trusted identity and group context.

What SEAL returned

SEAL returned a sealed refusal with code **SEAL-ROLE-DISALLOWED**, plus an audit trace reference, client policy reference, rule-basis evidence, and refusal integrity surfaces.

Why it matters

This proves refusal is not limited to one edge case. Even when identity is known and mapped, SEAL still blocks the action when the mapped role is structurally barred under policy.

Caption

This exhibit shows a governed refusal produced before the action left the firm. The artifact records who attempted the action, what was attempted, which policy context applied, and why the action was blocked.

Redacted public exhibit. Reviewer identity, matter-routing details, operational contact details, and live internal link destinations removed. Decision, policy, trace, and integrity references preserved.

Refusal C — Missing consent / authority condition not satisfied

Thinking OS™ – SEAL Enforcement Artifact
Case ID: b9e8c059-7d82-4bb5-9b57-2bb4040305a5
Artifact ID: 20260410123222-7c2063
Timestamp (UTC): 2026-04-10T12:32:18.155733Z

Status: Refusal record generated; see governance and runtime outcome below.
Reason: Consent not granted by Client ID; Client ID consent explicitly denied or structurally revoked; Policy reference: SEAL-CONSENT-001; Tenant consent regime: the firm designates one or more systems of record (for example, a consent registry, E-Sign platform, CRM, or matter system) as the source of truth for client authorization.; SEAL enforcement scope: evaluates only the consent signals and consent tokens-of-record that those systems send (for example, consent_id / consent_token_id, issuer, subject, scope such as vertical/motion, and expires_at), and refuses when configured policy requires consent but no valid consent token-of-record is present.; This explainer describes how SEAL applied firm-owned configuration to this request; it is not legal advice or a merits opinion.; Designed to support alignment with ABA Model Rule 5.5 (unauthorized practice of law).; Designed to support alignment with ISO 37301 (compliance management systems).; Designed to support alignment with FRCP Rule 11 (frivolous filings prohibition).; Governance requires explicit Client ID authorization before filing; Prevents unauthorized or premature submissions
Next step: No next-step instructions were provided to SEAL. Refer to your firm's escalation and filing procedures; SEAL does not prescribe remediation or timeframes.
Risk class: Not Classified
Enforcement: Enforce (runtime refusals are applied in-line with governance policy).

Unless otherwise noted, the fields in the table below were declared by the firm's own systems (IdP, matter/case systems, GRC). Entries shown as "Not Declared" indicate that no value was provided to SEAL at runtime; the runtime did not infer or alter those values.

Declared Role	Attorney
Declared Vertical	Administrative Law
Declared Scenario	Motion To Extend Time
Case Stage	Filing
Legal Environment	Administrative Law
Requested Turnaround	Standard
Refusal Code	SEAL-CONSENT-001
Severity	Block
Reviewer	[redacted]
Client ID	CLIENT-DEMO-MIDLAW-STRICT
Audit Trace ID	00539c78-382f-472b-ac48-c0a26bbafea7
Contact Advisory	Governance & Compliance / [redacted]
Advisory Action Link	[redacted]
Governance Reference	[redacted]
Auto-Reroute Triggered	No
Policy Mode (Client Regimen)	Client GRC Regime
Client Environment	Prod
Enforcement Posture	Enforce (runtime refusals are applied in-line with governance policy).
Policy Version	v1.0
Jurisdiction	US-VA

Governance Outcome Record

Outcome: Refusal

This section records the outcome and supporting inputs produced by the governance engine enforcing firm-owned policies. It is not legal advice or a legal opinion.

Summary (verbatim inputs): Consent not granted by Client ID; Client ID consent explicitly denied or structurally revoked; Policy reference: SEAL-CONSENT-001; Tenant consent regime: the firm designates one or more systems of record (for example, a consent registry, E-Sign platform, CRM, or matter system) as the source of truth for client authorization.; SEAL enforcement scope: evaluates only the consent signals and consent tokens-of-record that those systems send (for example, consent_id / consent_token_id, issuer, subject, scope such as vertical/motion, and expires_at), and refuses when configured policy requires consent but no valid consent token-of-record is present.; This explainer describes how SEAL applied firm-owned configuration to this request; it is not legal advice or a merits opinion.; Designed to support alignment with ABA Model Rule 5.5 (unauthorized practice of law).; Designed to support alignment with ISO 37301 (compliance management systems).; Designed to support alignment with FRCP Rule 11 (frivolous filings prohibition).; Governance requires explicit Client ID authorization before filing; Prevents unauthorized or premature submissions

Procedural Defects

- Consent not granted by Client ID
- Client ID consent explicitly denied or structurally revoked

Oversight Advisory

- Filing blocked under SEAL governance protocol; oversight review logged.

Rule Basis

- Policy reference: SEAL-CONSENT-001
- Tenant consent regime: the firm designates one or more systems of record (for example, a consent registry, E-Sign platform, CRM, or matter system) as the source of truth for client authorization.
- SEAL enforcement scope: evaluates only the consent signals and consent tokens-of-record that those systems send (for example, consent_id / consent_token_id, issuer, subject, scope such as vertical/motion, and expires_at), and refuses when configured policy requires consent but no valid consent token-of-record is present.
- This explainer describes how SEAL applied firm-owned configuration to this request; it is not legal advice or a merits opinion.
- Designed to support alignment with ABA Model Rule 5.5 (unauthorized practice of law).
- Designed to support alignment with ISO 37301 (compliance management systems).
- Designed to support alignment with FRCP Rule 11 (frivolous filings prohibition).

Rule-Basis Evidence & Authority

Rule-Basis Evidence

- Evidence Decision ID: `9e662e4d426747b5914aceff59beb47c`
- Policy Reference: `CLIENT-DEMO-MIDLAW-STRICT:mock-prod/administrative_law/motion_to_extend_time@v1.0`
- Consent requirement: SEAL-CONSENT-001 for administrative_law/motion_to_extend_time.
- Scope: administrative_law/motion_to_extend_time.
- Reviewer role: attorney (claims-mapped from groups).

Governance Summary (Short Form)

- Client ID consent explicitly denied or structurally revoked
- Governance requires explicit Client ID authorization before filing
- Prevents unauthorized or premature submissions

External Standards & Firm Mapping

This section is provided for regulators, insurers, and oversight functions that need to see how this refusal maps to the firm's external standards registry and compliance library.

Oversight Registry Reference: [redacted]
External Compliance Mapping: [redacted]

Artifact HTML Hash: sha256:4d9057e48f64ad5aabd1dd35913703b859b29668d30b4b1dc6a115268552d474 (sha256 over artifact contents above)
Governance Refusal Hash: sha256:3145cd73d3767b9448099b9d5d3001454bce4bdd0f8fca8bc272a7efb06129a3
Refusal Origin: SEAL Runtime Governance Layer
Issued By: Thinking OS™ — Enforcement Core (SEAL-Mode Enabled)
Chain of Custody: Refusal chain locked at runtime. Immutable and audit-ready. Field values not declared by input were substituted with explicit runtime fallbacks.
🔍 **Audit Echo:** Metadata logged for oversight and verification only.
Artifact Link: [redacted]

Scenario

A governed filing request was submitted under the strict runtime path for **Administrative Law / Motion To Extend Time**. The actor, motion, and timing posture were otherwise valid, but the consent condition required for that governed filing was not satisfied at the time of action.

What SEAL returned

SEAL returned a sealed refusal with code **SEAL-CONSENT-001**, plus an audit trace reference, policy reference, and refusal integrity surfaces.

Why it matters

This proves refusal behavior is not limited to role and authority. SEAL also blocks a governed filing when the required consent / authority condition for that action is missing.

Caption

This exhibit shows a governed refusal produced before the filing left the firm. The artifact records who attempted the action, what was attempted, which policy context applied, and why the request was blocked. Refusals are structured alerts tied to the firm's own rules and inputs, not post-hoc opinions.

Redacted public exhibit. Reviewer identity, matter-routing details, operational contact details, and live internal link destinations removed. Decision, policy, trace, and integrity references preserved.

Proof of Supervised Escalation

SEAL does not collapse everything into allow-or-block only. Where configured, it can route a governed action into supervised review or override with named accountability and proof. Public materials describe approve / refuse / supervised override as the three governed outcomes at the Commit Layer.

Thinking OS™ – SEAL Enforcement Artifact
Case ID: 4381ecb1-381c-4229-ba9f-e2d93d6380b7
Artifact ID: 20260413172056-4a25cd
Timestamp (UTC): 2026-04-13T17:20:54.679339Z

Status: Approval record generated; see runtime outcome below.
Reason: Approved. Identity verified (SSO:[redacted]). Scope validated: administrative_law • motion_for_summary_judgment per policy SEAL-OVERRIDE-APPROVED. Authority/evidence posture: authority=inline_authority (required); evidence=inline_evidence (required).
Next step: Follow your firm's implementation and record-keeping procedures; see detailed reasoning below.
Risk class: Not Classified
Enforcement: Enforce (runtime decisions are applied in-line with governance policy).
Governance decided: Refusal
Runtime decided: approval
Decision alignment: diverged
Control meaning: Baseline governance refused the action, but runtime approved it under supervisory override, and required downstream execution completed successfully.

Declared Role	Partner
Declared Vertical	Administrative Law
Declared Scenario	Motion for Summary Judgment
Case Stage	Prehearing Procedure
Legal Environment	Administrative Law
Requested Turnaround	Standard
Approval Code	SEAL-OVERRIDE-APPROVED
Reviewer	[redacted]
Client ID	CLIENT-DEMO-MIDLAW-OVERRIDE-HERO
Audit Trace ID	0f77d957-636d-4a1d-961b-a16e43a16fa0
Contact Advisory	[redacted]
Advisory Action Link	[redacted]
Governance Reference	[redacted]
Policy Mode (Client Regimen)	Client GRC Regime
Client Environment	Prod
Enforcement Posture	Enforce (runtime decisions are applied in-line with governance policy).
Policy Version	v1.0
Jurisdiction	US-VA
Policy Set	`CLIENT-DEMO-MIDLAW-OVERRIDE-HERO@v1.0`
Retention	`reg.standard` — TTL: 45 days
Identity Proof	SSO: [redacted]
Identity Source	no_claims
Role Map Version	Not Declared
Role Map Reference (Client-Owned)	idp=[redacted]
Consent-of-Record (Client-Owned)	Not Declared
Decision Stage	Vertical • Override • Approved
Decision Engine	[redacted]

Governance Outcome Record

Outcome: Approval

This record renders governance output and supporting metadata. It is not legal advice or a legal opinion.

Decision basis: Approved. Identity verified (SSO: [redacted]. Scope validated: administrative_law • motion_for_summary_judgment per policy SEAL-OVERRIDE-APPROVED. Authority/evidence posture: authority=inline_authority (required); evidence=inline_evidence (required).

Decision Inputs: Vertical: Administrative Law • Motion: Motion for Summary Judgment • Role: Partner • Jurisdiction: US-VA • Consent: true

Posture: Evidence: inline_evidence (required); Authority: inline_authority (required); Anti-Replay Nonce: required

Controls: Identity: pass • Role Map: pass • Vertical Allow: pass • Motion Allow: pass • Jurisdiction: US-VA • Evidence: required • Authority: required • Anti-Replay Nonce: required

Runtime Outcome & Execution Record

Governance Decision	Refusal
Pre-Execution Runtime Decision	approval
Baseline Governance Code	SEAL-ADVISORY-001
Final Runtime Decision	approval
Decision Alignment	diverged
Runtime Translation	Refusal → approval; baseline_refusal_code=SEAL-ADVISORY-001
Execution Receipt	

Status	ok
Attempted	True
OK	True
Hard Fail	False
Required	True
Mode	enforce
Execution Outcome	succeeded
Governance / Execution Alignment	aligned
Blocks Effective Completion	False
Control Meaning	Baseline governance refused the action, but runtime approved it under supervisory override, and required downstream execution completed successfully.

Executor Gate	**Status**	ok
	Attempted	True
	OK	True
	Hard Fail	False
	Required	True
	Mode	enforce
	Blocks Effective Completion	False
	Reason Code	Not Declared
	Reason	succeeded
	Control Meaning	Baseline governance refused the action, but runtime approved it under supervisory override, and required downstream execution completed successfully.
Plain-Language Control Meaning	Baseline governance refused the action, but runtime approved it under supervisory override, and required downstream execution completed successfully.	

Rule Basis & Authority

Rule-Basis Evidence

- Evidence Decision ID: `ed4b4abf5ffe44f9aa72cc0bfcbb70d5`
- Policy Reference: `CLIENT-DEMO-MIDLAW-OVERRIDE-HERO:mock-prod/administrative_law/motion_for_summary_judgment@v1.0-admin-msj`
- Scope: administrative_law/motion_for_summary_judgment.
- Motion requires supervisory review or override under current policy posture.
- Reviewer role derived from trusted claims/groups.

Rule-Basis Override:
• Parent Decision ID: `2337d396-34b3-4ea7-a288-931096980cfa`
• Override Kind: supervisory_override
• Override Reason: Supervising partner approved after advisory-required baseline decision.
• Override Actor: [redacted]

Authority Token

- Authority Decision ID: `ed4b4abf5ffe44f9aa72cc0bfcbb70d5`
- Applies To Decision ID: `2337d396-34b3-4ea7-a288-931096980cfa`
- Purpose: supervisory_override
- Scope: Vertical=administrative_law; Motion=motion_for_summary_judgment

Rule Basis

- Policy reference: SEAL-OVERRIDE-APPROVED
- Tenant override regime: certain baseline refusals may be superseded when designated supervisors apply a documented override under the firm's own policy framework.
- SEAL enforcement scope: records both the baseline governance refusal and the override decision; SEAL does not invent override policy, it verifies tenant evidence/authority signals and captures the override chain for audit.
- This explainer describes how SEAL applied firm-owned configuration to this request; it is not legal advice or a merits opinion.
- Designed to support alignment with ABA Model Rule 5.5 (unauthorized practice of law).
- Designed to support alignment with ISO 37301 (compliance management systems).
- Designed to support alignment with FRCP Rule 11 (frivolous filings prohibition).

Artifact HTML Hash: `sha256:2548754eb2481f043deea03d03539526d959c3f094f6b89415db3d42b6b22db8` (sha256 over artifact contents above).
Approval Origin: SEAL Runtime Governance Layer.
Governance Approval Hash: `983ee35edfb136604bc7722c1dc3215167b5360f446c6734131a2a76ed0c4a39`.
Issued By: Thinking OS™ — Enforcement Core (SEAL-Mode Enabled).
Chain of Custody: Approval chain locked at runtime. Immutable and audit-ready. Field values not declared by input were substituted with explicit runtime fallbacks.
Audit Echo: Metadata logged for oversight and verification only.
Artifact Link: [redacted]
Oversight Registry Reference: [redacted]
External Compliance Mapping: [redacted]
Policy Fingerprint: [redacted]
Runtime Config Snapshot: [redacted]

Scenario

A governed filing request for **Administrative Law / Motion for Summary Judgment** did not clear directly and was routed into supervised review. A supervising partner then submitted a linked override with documented supervisory authority and override evidence.

What SEAL returned

SEAL returned an override-flavored approval with a unique decision / trace reference, approval hash, linked baseline refusal context, and override metadata showing the supervising actor and basis for the override.

Why it matters

This proves SEAL does not collapse everything into allow-or-block only. It can preserve the original refusal, require named supervisory intervention, and record the override chain in an audit-ready artifact before execution completes.

Redacted public exhibit. Reviewer identity, matter-routing details, operational contact details, and live internal link destinations removed. Decision, policy, trace, and integrity references preserved.

Execution Receipts and Artifacts Tell the Same Story

This exhibit shows that SEAL is not a static artifact generator. A governed request was received, a decision was returned, a sealed artifact was emitted, and the downstream handling event reflected the same governed outcome.

Block 1 — Governed request received

A filing request for **Administrative Law / Motion To Extend Time** entered the strict runtime path with a valid attorney actor, consent present, and sufficient time to deadline.

Declared Role	Attorney
Declared Vertical	Administrative Law
Declared Scenario	Motion to Extend Time
Case Stage	Filing
Client ID	CLIENT-DEMO-MIDLAW-STRICT
Deadline At	2026-04-15T22:42:25Z
Hours To Deadline	47.99791593611111

Block 2 — Decision returned

SEAL returned a governed approval with a unique trace reference and approval code for that request.

Approval Code	SEAL-APP-ALLOWED-001
Client ID	CLIENT-DEMO-MIDLAW-STRICT
Audit Trace ID	f5006e4f-387a-4e43-bac8-f512f10f5d1e
Governance Decision	approval
Pre-Execution Runtime Decision	approval
Decision Alignment	aligned

Block 3 — Artifact emitted

The approval generated a sealed artifact with its own integrity-verifiable approval hash linked to the same governed decision.

Artifact HTML Hash: `sha256:7a93187a6f37c65ff6a6672257f4002fcaf1f97c98aceae2b1a0b7facadea93c` (sha256 over artifact contents above).
Approval Origin: SEAL Runtime Governance Layer.
Governance Approval Hash: `23cb80f9b12cf4bd3fdb2740d32d5902d599e7fb091ed0309d13ce8b1bf62d0b.`
[redacted]
Chain of Custody: Approval chain locked at runtime. Immutable and audit-ready. Field values not declared by input were substituted with explicit runtime fallbacks.

Block 4 — Downstream handling event

The execution receipt shows that downstream handling was attempted and succeeded, with alignment between the governed decision and execution outcome.

Runtime Outcome & Execution Record

Governance Decision	approval
Final Runtime Decision	approval
Execution Receipt	**Status**: ok **Attempted**: True **OK**: True **Execution Outcome**: succeeded **Governance / Execution Alignment**: aligned **Endpoint Attempted**: True **Endpoint OK**: True **Endpoint HTTP Status**: 200
Plain-Language Control Meaning	Governance approved and required downstream execution completed successfully.

Redacted public exhibit. Reviewer identity, matter-routing details, operational contact details, and live internal link destinations removed. Decision, policy, trace, and integrity references preserved.

Scoped Non-Bypassability for the Demo Workflow

For the scoped workflow, the final submit boundary is gated: valid downstream action depends on a governed outcome from SEAL. Designated workflows only proceed once SEAL has approved.

Block 1 — Approved path through SEAL

Thinking OS™ – SEAL Enforcement Artifact
Case ID: [redacted]
Artifact ID: [redacted]
Timestamp (UTC): 2026-04-14T17:17:26.746947Z

Status: Approval record generated; see runtime outcome below.
Reason: Approved. Identity verified (SSO:[redacted]. Scope validated: administrative_law • motion_to_extend_time per policy SEAL-APP-ALLOWED-001. Authority/evidence posture: authority=inline_authority (required); evidence=inline_evidence (required).
Next step: Follow your firm's implementation and record-keeping procedures; see detailed reasoning below.
Risk class: Not Classified
Enforcement: Enforce (runtime decisions are applied in-line with governance policy).
Governance decided: approval
Runtime decided: approval
Decision alignment: aligned
Control meaning: Governance approved and required downstream execution completed successfully.

Declared Role	Attorney
Declared Vertical	Administrative Law
Declared Scenario	Motion to Extend Time
Case Stage	Filing
Audit Trace ID	c7255b8e-15a3-4860-a525-dba8667cfa69
Approval Code	SEAL-APP-ALLOWED-001

Runtime Outcome & Execution Record

Governance Decision	approval	
Final Runtime Decision	approval	
Execution Receipt	**Status**	ok
	Execution Outcome	succeeded
	Governance / Execution Alignment	aligned
	Endpoint HTTP Status	200
Executor Gate	**Blocks Effective Completion**	False

Approval Origin: [redacted]
Governance Approval Hash: cf71efe9cc5dbde0a1fa3c6a99e1367a6d52a4c3157153da4e9a3e45789a263e.
Issued By: [redacted]
Chain of Custody: Approval chain locked at runtime. Immutable and audit-ready. Field values not declared by input were substituted with explicit runtime fallbacks.

Approved path through SEAL

A governed filing request for **Administrative Law / Motion To Extend Time** passed through SEAL and reached the downstream execution path only after governed approval. The approval artifact and execution receipt share the same decision story: **SEAL-APP-ALLOWED-001**, audit trace **c7255b8e-15a3-4860-a525-dba8667cfa69**, execution outcome **succeeded**, and alignment **aligned**.

Block 2 — Direct call attempt to commit target

A direct forged call to the downstream commit target was attempted without a valid governed path through SEAL. The downstream gate rejected the call.

- Outcome: **rejected**
- Reason: **invalid governed path**
- Deterministic: **true**
- OK: **False**

Block 3 — Deterministic rejection on repeat

The same forged direct call was repeated and rejected the same way both times. This shows the downstream gate is deterministic, not discretionary.

- Attempt 1 Status: **401**
- Attempt 1 Reason: **hmac-signature_mismatch**
- Attempt 2 Status: **401**
- Attempt 2 Reason: **hmac-signature_mismatch**
- Deterministic: **True**

Bottom takeaway

Valid downstream action depends on a governed outcome from SEAL; direct forged calls to the commit target are rejected deterministically.

Who Owns the Rules, the Runtime, and the Proof

The firm owns	Thinking OS is responsible for
• policies and authority rules • identity / role sources • matter and workflow context • supervision model • workflow routing scope • retention, use, and disclosure of decision artifacts and matter records	• operation of the governance runtime within agreed scope • faithful enforcement of configured conditions • decision artifact generation • runtime security, availability, and isolation

Caption

Public materials are explicit: the firm retains responsibility for policies, people, authority, workflow scope, and the use of resulting records. Thinking OS is responsible for the correct functioning of the SEAL runtime within agreed scope and for producing reviewable decision artifacts. SEAL does not supply legal judgment or replace the firm's GRC, identity, or matter systems.

What This Runtime Is Not

SEAL is a pre-execution authority gate for governed legal actions. It enforces firm-owned rules at the point of action and produces sealed decision artifacts. It does not replace legal judgment, attorney supervision, or the firm's own systems of record.

SEAL does not:

- draft, edit, sign, or file legal documents
- provide legal advice or choose litigation strategy
- replace lawyers, supervisors, or ethics counsel
- replace GRC, identity, matter, or case-management systems
- become the system of record for matters or filings
- determine legal merits or ethical safety on its own

SEAL can refuse; it cannot file.

Approvals show that configured governance conditions were satisfied at the moment of action. They do not certify strategy, merits, ethics, or professional judgment. Attorneys remain responsible for all decisions, filings, and communications.

Public evaluation reference. Redacted.

Describes evaluator-visible behavior and evidence surfaces only; no non-public runtime details are included.

For information only. Not legal advice.