

Your Agent's Prompt Is Not Its Mandate

A detailed prompt remains conversational context. Consequential financial authority needs a separate, machine-checkable mandate evaluated at the tool boundary for every proposed action.

HINTS, TIPS & TRICKS

- Represent observe, recommend, draft, stage and execute as separate permissions.
- Return a reason code and evidence for every boundary denial.
- Issue fresh authority for exceptions rather than reinterpreting the rule.

OPERATOR CHECKLIST

- Name authoriser, agent and purpose.
- Scope account, tool and counterparties.
- Set action level, limits and expiry.
- Require source and approval evidence.
- Rehearse handoff, denial and revocation.

COPY-READY PROMPT

Create a seven-line mandate for [agent action]: authority, purpose, scope, action level, limits, evidence and stop path. Then propose four boundary tests covering wrong account, excessive amount, expired authority and missing approval. State the deterministic denial and human handoff expected for each.

SOURCE & PROVENANCE

Article claims: The issue discusses financial tools exposed to agents and protocol approaches that preserve evidence of user intent.

Operational guidance: The seven-line mandate, negative tests and handoff rehearsal are guidance; controls still depend on enforcement.

Canonical package: 2026-08-21 · payload, final article, source digest, signal scan and section audit.