ACL — Fraud Firewall Use Case (at-a-glance)

Scenario	Traditional outcome	ACL outcome (pre-settlement)
Hacked hot wallet (exchange drain)	Funds leave, then you're chasing on-chain breadcrumbs (usually unrecoverable).	**Blocked before settlement** when source/destination is flagged; event **immutably logged**.
Phishing / scam address	User sends to a known bad address; only discovered after loss.	Transfer to **blacklisted address prevented**; sender sees clear message; **audit trail recorded**.
Suspicious large transfer (e.g., $10M from new wallet)	Clears first, investigated later; if fraud, the money's gone.	**Soft hold / challenge**: pause, request extra verification or secondary approval; **then** settle or reject.
Wash trading / layering pattern	Sophisticated rings complete cycles before analytics flag it.	**Pattern intercepted** via simulation rules (velocity/graph signals); **block or hold** prior to finality.

How flagged transactions are handled (configurable)

- **Hard block** (critical red flags like sanctions): reject + log.
- **Soft hold / challenge** (gray zones): pause, request extra data/approval, then clear or reject.
- **Auto-remediation**: if missing fields are supplied within window, transaction auto-clears.

UX reality

- **99%+** of normal transactions pass instantly. Only edge cases hit a hold.
- Every decision (pass/hold/reject) is **tamper-proof logged** for regulator trust.

"ACL is a circuit breaker: invisible when things are normal, essential when they're not. It stops theft and fraud **before** settlement and proves it with an immutable trail."