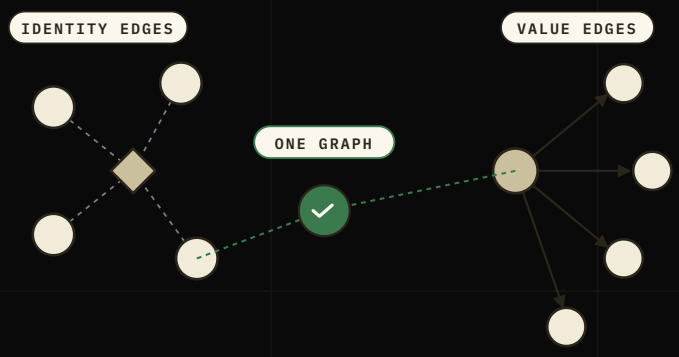
LOCI

TECHNICAL BRIEF · GRAPH INTELLIGENCE

The fraud isn’t in the accounts. It’s between them.

Fraud ring intelligence on one entity intelligence graph, fed by value movement and by identity, that accumulates with every confirmed case, with an inspectable trail instead of an opaque score.



one graph, two kinds of edge
the ring lives in the edges

THE GRAPH PROBLEM

A ring hides between the accounts

A fraud ring is a set of accounts operated toward a common end, such as bonus farming, laundering, or coordinated account takeover, that your controls treat as independent. Per-account and per-transaction scoring evaluates each node on its own, so a ring whose individual accounts each stay under threshold passes clean.

WHY SINGLE-NODE SCORING FAILS

The fraud is not in the accounts. It is in the edges between them. A ring is a connected subgraph: a cluster joined by relationships that should not exist between strangers. Detection is therefore a graph problem, not a scoring problem.

The entity intelligence graph

Loci keeps one relationship graph keyed on the entity, the entity intelligence graph, with a single kind of node and edges from two independent sources.

VALUE MOVEMENT

How value moves. Every transaction is a directed edge, weighted by amount, timestamped, and able to carry a fraud label. Present for every customer. Answers what is happening.

IDENTITY + BEHAVIOR

Who is behind it. Edges express that two accounts share a device, a behavioral signature, or a session lineage. An AccessGate opt-in module: without it, simply fewer edge types on the same graph. Answers who is actually there.

ONE GRAPH, NOT TWO

Treating this as one graph rather than two is the whole point. The two edge sources cover each other's blind spots, the same machinery reads them together, and every confirmed case writes back into the same structure: a single, sharpening picture, not two datasets joined at query time.

STRUCTURAL SIGNALS

What the graph can see

From value movement

Connected components partition the graph into the maximal sets of accounts reachable through transaction edges. A large, dense component among accounts that claim to be unrelated is unusual. **Centrality** ranks the accounts activity revolves around, a collector or a funder, using true degree centrality normalized to a time window (typically 30 days) so a short-lived, high-throughput account is not mistaken for a structural hub. Removing a central hub disconnects the ring.

Two **motifs** are especially diagnostic:

FAN-OUT (STARBURST)
One account sending to many distinct counterparties in a short window (for example, five or more transfers inside 30 minutes). A distribution point spraying funds across a ring.

PASS-THROUGH (MULE)
Money in roughly equal to money out within a short window, leaving little residual (for example, at least 80 percent of inflow forwarded). An account moving other people's money.

From identity and behavior

Device-sharing edges record which accounts appear on a device fingerprint; the edge weight reflects how exclusive the sharing is (two accounts is weaker evidence than twenty). **Behavioral-similarity edges** compare per-account interaction dynamics; high similarity between accounts that claim to be different people is strong evidence, because emails, cards, and IPs are cheap to rotate while motor behavior is not. **Session lineage** ties an account's events into one verifiable thread, so device and behavioral observations attach to the same session.

NO SINGLE SIGNAL IS A VERDICT

Behavioral similarity is weighed as corroborating evidence, not asserted as sole proof. It is one of the harder signals for a ring to fake, and it is strongest when the device and value-movement signals agree.

DISCRIMINATION

Family or fraud ring?

Shared infrastructure is normal. Households share tablets; offices share workstations. Treating a shared device as fraud outright generates false positives at a rate that gets network detection switched off. The graph resolves the ambiguity by combining edges rather than reacting to any single one.

POINTS TOWARD A RING	POINTS TOWARD LEGITIMATE SHARING
A device behind many accounts (5+)	A small, stable set of accounts
Near-identical behavior across accounts claiming to be different people	Behavioral differences consistent with genuinely separate people
Devices added within minutes (scripted)	Devices added gradually over time
Accounts span several countries quickly	Consistent geography
Value-movement edges show fan-out or pass-through	Ordinary, unpatterned activity

INCONCLUSIVE BY DESIGN

When evidence is thin, from too few profiles or too little history, the verdict is inconclusive rather than a default to trusted or fraud. Thin data should earn neither trust nor a verdict; it warrants continued monitoring. The online edition lets you toggle this evidence yourself: runloci.com/brief/fraud-ring-detection.

Reading the graph from both sides

A laundering ring that layers through freshly provisioned, unshared devices leaves no identity edges, but its motifs show in its value movement. A promo-abuse ring that never moves money between its accounts leaves no transaction edges, but its shared devices and near-identical behavior show in its identity edges. A ring that evades one is unlikely to evade both at once.

CORROBORATION IS A CONJUNCTION

A cluster connected by transaction motifs and by shared-device or behavioral edges is a stronger finding than either alone, and it carries an inspectable trail: the accounts, the device fingerprints, the transactions, and the motif that fired. The transaction edges show what is happening; the identity edges show who is behind it.

The check runs automatically: a cluster flagged from one kind of edge is tested against the other, and the findings both confirm are the strongest of all. One entity, seen from two independent angles at once, on one graph.

COMPOUNDING + LIMITS

An asset that compounds, honest about its edges

RELATIONSHIP INTELLIGENCE THAT PERSISTS

Unlike systems that evaluate isolated events, Loci persists relationship intelligence between entities. Every confirmed investigation permanently enriches the graph, allowing future attacks to be recognized from their infrastructure rather than from a single transaction.

Confirmed outcomes feed back into the graph. Confirming an account as fraud flips the label on its transaction edges and triggers recomputation of the surrounding neighborhood, so the cluster is scored with that knowledge rather than from scratch. Entity and device standing is a running posterior: each observation updates a prior instead of replacing it. A confirmed ring's signature becomes a pattern the system matches faster on recurrence.

Worked examples

Promo and bonus farming. Forty accounts sign up for a referral bonus, each with a distinct email; per-account checks clear most. Value movement shows little, because they do not pay each other. But on the identity edges the forty accounts collapse onto six device fingerprints with near-identical behavior, several added within minutes. Flagged from the identity side, the bonus held before the fortieth payout. The family with one tablet and three accounts stays inconclusive and is not touched.

Mule network. A layer of accounts receives inbound transfers and forwards roughly 90 percent within the hour. Each, alone, looks like an active customer. The pass-through motif fires across the layer, connected components tie them to a common funder showing fan-out, and centrality identifies the collector. Even with fresh, unshared devices and no identity edges, the value-movement edges carry the finding.

LIMITS, STATED PLAINLY

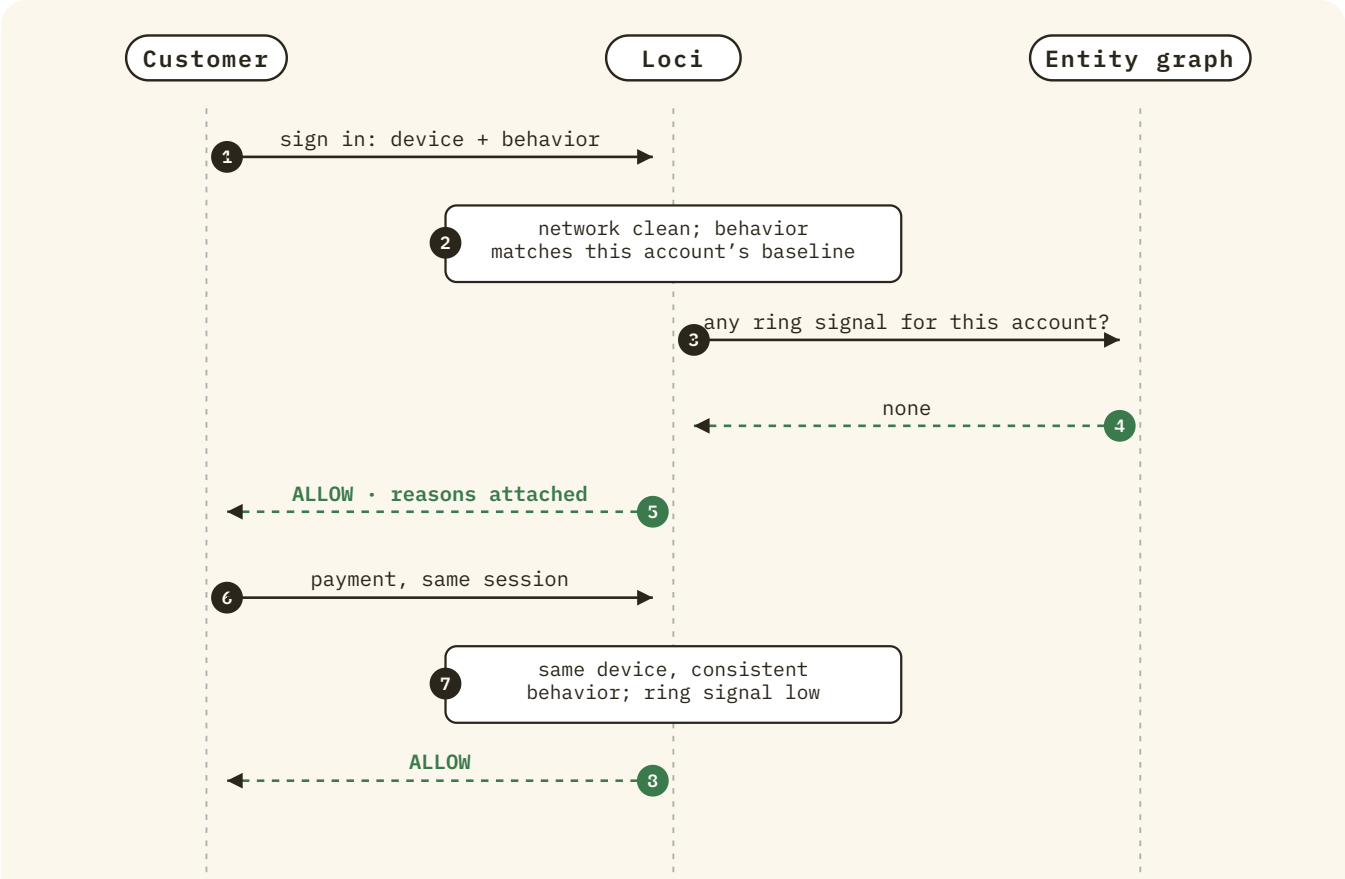
No transactions, no value-movement motifs. No AccessGate, no identity edges (value-movement detection still runs, single-sided). Thin evidence yields inconclusive by design. Per-tenant isolation is deliberate: each institution's graph is its own, forgoing any cross-institution signal in exchange for data sovereignty.

The transaction edges show what is happening.
The identity edges show who is behind it.

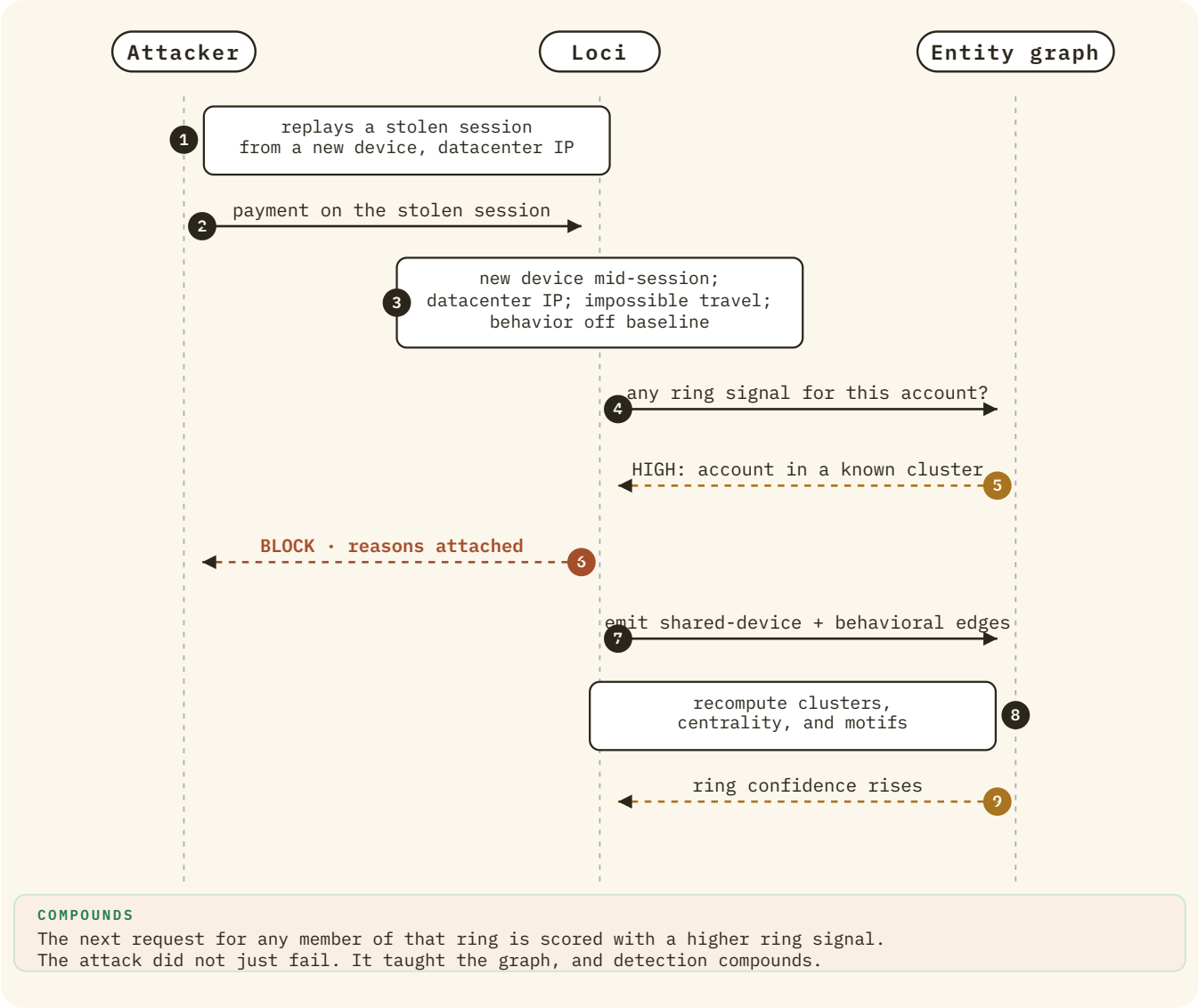
APPENDIX

Example data flow

Two illustrative sequences show how a single decision draws on the graph, and how a blocked attack feeds back into it. They are conceptual and simplified; production naming, parameters, and internal steps are omitted.



A legitimate customer. The session is allowed, and the graph is unchanged.



A stolen-session replay. The attempt is blocked, and it makes the graph smarter for next time.

About Loci

Loci is the intelligence infrastructure for modern finance. Loci empowers every defender, analyst, and enterprise system to operate with confidence, clarity, and adaptive insight. With Loci, everyone becomes intelligent.

SEE IT ON YOUR GRAPH

A walkthrough of ring detection on your own transaction and device data, from a single suspicious node to the cluster around it. Toggle the evidence yourself at runloci.com/brief/fraud-ring-detection.

LOCI FRAUD AI · TECHNICAL BRIEF runloci.com · sales@runloci.com