Murphy

Collateral Negligence

Control State Replaces Trust

March 2026

Dedicated to: MISMO, CREFC, and LSTA.

I’ve spent twenty years connecting financial systems through APIs.

Everything in this document is based on publicly available information.

Collateral-egligence.com
Updated March 31, 2026
New York, New York

Win without trying.

In June 2024, I was visiting family. Everyone in San Francisco was building retrieval augmented generation systems that summer. For the first time, large language models could query private corpora before answering. Early users called it a second brain. That month, a plugin turned my note taking app, Obsidian, into one of those systems. I had years of CRM data sitting in a vault, notes, invoices, supplier records. I installed it and let it read everything.

I had built technology my whole life. One of those companies was in AI. None of them did this. The system was not returning rows from a table. It was making connections. It pulled together notes written years apart, cross referenced a supplier against two audits, and surfaced a timing overlap. At moments it made logical inferences without prompting. It felt less like software and more like a colleague who had read everything I had ever written and remembered all of it at once.

Unbeknownst to anyone in 2024, more than five billion dollars of collateral fraud had already begun. The first forensic accountants would quietly arrive at First Brands that same summer. Then MFS. Then Stenn. Then Tricolor. The fraud was not new. The controls were finally old enough to fail publicly. And the technology to catch it was already running inside a note taking app.

Let me tell you what is happening now.

Contents

Contents

Every scaled asset class standardized its data before it scaled its funding market.

DISLOCATION

I. $5B in Eighteen Months

Four collapses made the gap visible.

Late 2025 and early 2026 ended the fiction that collateral verification was a back office nuisance. Four separate failures surfaced through fabricated invoices, duplicate collateral, falsified portfolio data, or diverted cash. The common feature was not ordinary credit deterioration. It was operational deception inside slow, bilateral control systems. More than five billion surfaced across First Brands, MFS, Stenn, and Tricolor in eighteen months. Then the same market that financed those assets gated liquidity. Fraud arrived first. Repricing followed.

[PLACEHOLDER FOR IMAGE: p06_opener1_fraud.png]

First Brands: $2.3 billion in forged receivables, multiple duplicate pledges, $1.9 billion not remitted to lenders.
MFS: £930 million plus shortfall, connected borrowers, duplicate collateral, diverted income streams.
Stenn: $700 million plus hole, shell company invoices mimicking blue chip buyers, roughly 10 percent recovery.
Tricolor: $370 million plus, falsified portfolio data, duplicate auto loan pledges across lenders.

Sources: Bloomberg, Reuters, DOJ indictments, FCA enforcement proceedings, court filings.

Semi liquid structures stopped acting liquid.

Redemption gates exposed the liquidity mismatch.

Once the fraud cycle reached the market, investor cash stopped moving as advertised. More than $150 billion across major retail private credit vehicles hit withdrawal limits in Q1 2026. The important point is not retail sentiment. It is structure. These vehicles promised periodic liquidity against portfolios whose underlying assets were already showing stress, opacity, and concentrated sector exposure. When redemption pressure arrived, the gates showed what the market already knew: the collateral stack was being repriced faster than managers could sell or certify it.

[PLACEHOLDER FOR IMAGE: p07_opener2_gating.png]

Goldman Sachs projected $45 to $70 billion of asset shrinkage over two years. More than $4.6 billion remained trapped behind withdrawal limits.

Sources: Goldman Sachs, Bloomberg, company letters, SEC filings.

The gated funds owned the same stress.

Hidden concentration, weaker cash interest, and illiquidity surfaced together.

Public reporting exposed a second layer of fragility. Several of the largest retail private credit funds carried materially more software exposure than public filings implied. The same group, Blue Owl, Blackstone, Ares, Apollo, also appeared in the gating cycle. Fitch put the United States private credit default rate at 9.2 percent for full year 2025, a record. Reuters then reported that more than a third of software borrower agreements included payment in kind options by the end of 2025. Hidden concentration, weaker cash interest, and gated liquidity all showed up together.

[PLACEHOLDER FOR IMAGE: p08_opener3_software.png]

This was not a narrow sector problem. It was a disclosure problem, a control problem, and a liquidity problem at the same time.

Sources: Wall Street Journal, Reuters, Fitch.

II. Hours vs. Days

Origination moved daily. Verification stayed monthly.

The growth engine of modern asset backed finance is forward flow, programmatic capital commitments that buy receivables, consumer loans, and merchant advances every day. These commitments scale because the operating surface is tight. One platform. One warehouse line. Fast decisioning. Digital identity at application. Daily purchasing works when the asset is normalized at creation and the lender has continuous sight into performance. The same model was then carried into enterprise receivables without rebuilding the control layer. That is where the gap opened.

Forward flow was not the problem. Fast origination paired with slow verification was the problem.

High velocity worked when the system was closed.

Consumer forward flow proved speed under a coherent stack.

Consumer forward flow already proved that institutional capital will fund machine speed origination when the operational stack is coherent. Large commitments, Liberty Mutual and Affirm, KKR PIMCO and Harley Davidson, Sixth Street and Affirm, Blue Owl and LendingClub, all sit on cleaner identity, cleaner servicing, and tighter warehouse structure. Double pledge risk is structurally harder when one platform originates, one lender funds, and one system of record governs the asset.

[PLACEHOLDER FOR IMAGE: p10_consumer_forward_flow.png]

The lesson is not that speed is dangerous. The lesson is that speed without shared verification is dangerous.

Sources: company announcements, press releases, PitchBook.

The fraud happened in the time delta.

Enterprise receivables kept the speed and lost the closed loop.

Enterprise receivables kept the speed and lost the closed loop. Assets could be purchased in hours while control infrastructure still refreshed on weekly, monthly, or quarterly cycles. Borrowing base certificates and field exams were designed for slower markets. A duplicate invoice submitted to two capital providers a few days apart could clear both portfolios before either review cycle ran. That is why the failure mode repeated across cases. The fraud did not beat the controls. It passed through the space the controls left open.

[PLACEHOLDER FOR IMAGE: p11_verification_latency.png]

When origination runs at hours and verification runs at days or months, the attack surface is temporal before it is legal.

Sources: industry practice, MINT architecture.

III. The Same Invoice Twice

Bilateral audits never see shared fraud.

Double pledging is the recurring failure mode because the market still audits in isolation. In enterprise receivables, the same invoice can be presented to multiple capital providers, each operating inside a bilateral silo, each running its own collateral exam against its own borrowing base certificate, each unable to see the others. The identifiers may match, the economics may be impossible, the cash path may diverge, and none of it becomes visible until after funding.

[PLACEHOLDER FOR IMAGE: p12_enterprise_forward_flow.png]

Consumer forward flow solved for velocity because the infrastructure constrained the asset. Enterprise forward flow kept the velocity and left uniqueness unresolved. One lender sees one pool. No lender sees the market.

Sources: DOJ indictments, FCA enforcement proceedings, court filings.

IV. Capital Moved First

Demand moved before product existed.

Institutional capital did not wait for a finished category. It moved first. The allocators closest to the risk began building data layers, internal monitoring systems, and verification requirements before an independent control state product existed in the market. ICE launched Private Credit Intelligence with Apollo as anchor partner. Victory Park required daily asset level monitoring. CNO committed capital conditioned on continuous monitoring. Janus Henderson framed winners around transparency, data precision, and disciplined execution. The buy side signaled the requirement before the sell side product was mature.

[PLACEHOLDER FOR IMAGE: p13_response.png]

The requirement became explicit before the category existed.

Sources: Reuters, Janus Henderson, Victory Park, ICE Apollo press release.

Sovereign and insurance allocators moved at the same time.

Monitoring conditions migrated into capital commitments.

Abu Dhabi backed new private credit infrastructure through Apollo Atlas SP. Mubadala expanded structured credit partnerships. Ontario Teachers continued to enlarge private credit as a permanent allocation. Insurance capital made the same turn. CNO wrote a monitoring condition directly into capital commitments.

This matters because it changes the budget conversation. Once a board sees fraud, gating, and allocator conditions in the same quarter, collateral monitoring stops looking like optional software. It becomes deployment infrastructure.

Sources: public filings, press releases, institutional partnership announcements.

V. The Only Structural Defense

Six requirements emerged from the wreckage.

Every major collateral failure since 2024 exploited the same missing controls. Slow reporting. Borrower supplied evidence. Weak entity resolution. Weak lien visibility. Weak cash confirmation. No cross program duplicate detection. The failures were different in surface details but consistent in operating logic. That consistency matters because it turns post mortems into product requirements. The market no longer needs a general warning about fraud. It needs a control architecture that answers the same questions before every purchase.

Before capital buys the asset, can the claim be independently resolved, legally cleared, cash traced, and cross checked for uniqueness?

Ledger, legal, cash, collision.

Four control domains govern asset integrity.

The control architecture collapses into four domains. Ledger asks whether the receivable exists, matches the buyer record, and clears approval logic. Legal asks whether the claim is encumbered, mistitled, or attached to the wrong entity. Cash asks whether the payment path, bank account, and remittance pattern validate the asset. Collision asks whether the same claim, or a materially identical claim, already sits inside another program.

At minimum the system now runs onboarding lien search, continuous UCC monitoring, supplier-side ERP forensics, remittance routing checks, and supplier attestations before capital buys the asset.

Cross program visibility is the missing control.

A collision registry changes the geometry of the problem.

The market has no shared duplicate detection layer. That is why every lender can be correct inside its own file and wrong at the portfolio level. A collision registry changes the geometry of the problem. With one program there is no cross program visibility. With many programs, detection coverage compounds quickly. Once the network reaches critical mass, duplicate claims become harder to finance than to originate.

[PLACEHOLDER FOR IMAGE: p17_collision_detection.png]

This is the difference between periodic auditing and market level uniqueness control. The first finds losses after the fact. The second blocks the asset before funding.

Sources: DOJ indictments, FCA enforcement proceedings, court filings, UCC Article 9, OFAC lists, MINT architecture.

VI. Everything Converged in 2026

Standards, rails, and execution aligned.

Three infrastructure changes that had developed separately suddenly became mutually reinforcing. Structured remittance data made payments legible. Instant payment rails made confirmation fast enough to matter operationally. ERP execution surfaces made it possible to reconcile business events inside live systems rather than in quarterly exams. None of these changes alone solved collateral verification. Together they created the first credible technical foundation for continuous verification at machine speed.

[PLACEHOLDER FOR IMAGE: p18_convergence.png]

This section is the closed loop. Data, confirmation, and execution now exist in the same operating window.

Sources: SWIFT, Federal Reserve, Oracle, MINT synthesis.

Pipe 1: Structured remittance became evidence.

ISO 20022 turned payment metadata into an operating signal.

For years, payment flows carried the money but not enough structured context to verify the asset that generated it. ISO 20022 changes that. Invoice references, amounts, dates, routing details, adjustments, and remittance context can now travel in structured form. That matters because fraud often hides in the space between the commercial document and the payment that settles it. Once remittance becomes machine readable, payment messages stop being accounting residue and become evidence.

Structured remittance does not eliminate fraud. It makes reconciliation precise enough for software to participate in the control loop.

Pipe 2: Confirmation moved to real time.

Settlement latency compressed from batch delay to operational immediacy.

A confirmation signal that arrives too late is a report, not a control. Instant payment rails change that timing. FedNow matters less as a consumer payments story than as proof that core domestic payment confirmation can now move fast enough to matter in daily operating systems. The same market that was still funding against monthly borrowing base cycles now has access to payment networks designed for real time message exchange, immediate status visibility, and operational automation.

Speed alone is not a control. But without speed, the rest of the control stack cannot close.

Pipe 3: ERP execution became a control surface.

Business systems now expose live state instead of periodic reports.

The final shift happened inside enterprise software. ERP stopped behaving only as a system of record and started behaving like an execution surface. Oracle’s agentic application push made the point explicit: live systems can now orchestrate actions, return structured state, and coordinate automated workflows inside the transactional environment. For collateral verification, that means receivables no longer have to be understood from files exported long after the fact. They can be checked against the state transitions that create, route, approve, and settle them.

Execution moved closer to the ledger. That is what makes continuous verification technically credible.

The closed loop.

Creation, pledge, payment, and confirmation can now reconcile continuously.

The market used to treat creation, underwriting, payment, and verification as separate phases. That assumption is breaking. The underlying business event now creates machine-readable state. The payment rail returns structured confirmation. The enterprise system records each transition. The verification layer can evaluate the asset before purchase, then continue to monitor it until collection. That is the closed loop the market lacked in every recent fraud case.

The claim is simple. The architecture that used to be impossible is now executable.

UNDERWRITING

VII. Two Properties

External evidence makes the asset real.

This convergence created two capabilities that did not previously exist together. First, external evidence now scales. Public lien records, sanctions data, bank validation, remittance histories, and supplier-authorized portal states can be pulled into a verification pipeline as structured signals instead of manual exhibits. Second, machine reading can now extract contradictions from the messy commercial record, invoices, purchase orders, amendments, ship notices, remittances, and correspondence, before a human examiner would ever review the file. One capability makes the asset real. The other makes the system adaptive.

[PLACEHOLDER FOR IMAGE: p23_two_properties.png]

Six reported fields enter. A verified instrument with evidence lineage, control state, and integrity relevance exits.

Sources: MINT verification schema, UCC data, sanctions lists, remittance data, model-assisted document reading.

VIII. Resolve the Receivable

MINT turns reported tapes into a control state.

A fund begins with a tape. MINT begins with proof. The tape says an invoice exists. The system asks whether it can be independently confirmed across ledger, legal, cash, and collision. Every entity is resolved. Every lien is checked. Every bank path is validated. Every sanction screen is cleared. Every duplicate is tested across programs. The output is not a spreadsheet row. It is a verified receivable with evidence lineage, control state, pricing relevance, and eligibility logic already attached.

[PLACEHOLDER FOR IMAGE: p24_resolve_receivable.png]

Advance rates and reserves calibrate to verification confidence. Full confirmation clears tighter pricing. Partial confirmation clears only at tighter controls or lower advance.

Sources: MINT process architecture, supplier-side verification memo, UCC and remittance controls.

IX. Capital Infrastructure for Machines

As cognition becomes cheap, value concentrates in the control layer.

Artificial intelligence changed the cost of cognition before finance changed the cost of trust. Coding, analysis, and research are becoming abundant inputs. In asset-backed finance, the scarce asset is no longer interpretation. It is sanctioned access to definitive enterprise state and the capital machinery that can act on it. Machines cannot fund against PDFs, monthly certificates, or manually interpreted exceptions. They need verified data, executable policy, and capital paths that clear automatically once the asset is real. MINT is not receivables software beside the capital stack. It is capital infrastructure for machines.

[PLACEHOLDER FOR IMAGE: p25_mint_context_shift.png]

Enterprise automation, trade fragmentation, and private credit created a capital infrastructure gap. This page proves why the category must exist.

Sources: MINT Capital Infrastructure for Machines memo.

X. The Integration Void

Authorized access now reaches definitive enterprise state.

The central market failure is not lack of software. It is lack of direct integration between enterprise truth and deployed capital. Historically, definitive buyer state sat behind portals, bilateral relationships, and long integration queues. That assumption is breaking. Supplier-authorized access to buyer-facing records, scheduled exports, and live APIs where available now provides enough definitive state to verify issuance, routing, approval, remittance, and payment without waiting for a monolithic buyer-side integration.

[PLACEHOLDER FOR IMAGE: p26_integration_void_v2.png]

Sanctioned access only. No full buyer-side ERP ownership required.

Sources: MINT Capital Infrastructure for Machines memo, supplier-side verification architecture.

XI. Agents Need Collateral Infrastructure

An agent cannot underwrite from a dashboard.

The next user of collateral infrastructure will not be an analyst. It will be an agent executing inside a policy loop. An agent needs callable tools, deterministic outputs, structured state, and a full audit trail for every action. That is why MINT’s surface matters. Tape scan, entity resolution, lien search, collision detection, compliance checks, monitoring, certification, reporting, lane analysis. The system returns structured JSON, executes the verification pipeline, then blocks, certifies, or escalates. Once that exists, collateral integrity moves from dashboard workflow to machine infrastructure.

[PLACEHOLDER FOR IMAGE: p25_dashboard_to_toolcall.png]

50+ tools, 13 checkpoints, 4 control domains, structured JSON, full audit trail.

Sources: MINT for Agents HTML, MINT CLI notes.

XII. The Layer Is Open

No incumbent owns the independent control state across ledger, legal, cash, and collision.

Existing platforms each solve a fragment. Supply chain finance systems move money. Lenders underwrite inside their own portfolio. Analytics vendors summarize data already in hand. Auditors inspect after the fact. None produces an independent control state before each purchase across the four domains that actually matter. That missing layer is the category. It sits between reported data and deployed capital. It compounds as more tapes are scanned, more entities are resolved, and more duplicates are caught across programs.

[PLACEHOLDER FOR IMAGE: p26_layer_is_open.png]

The defining company will be the one that establishes the control state.

Sources: market landscape analysis, MINT position memo.

XIII. Capital Attaches to Lanes

Historical tape proves the lane. Continuous monitoring preserves it.

The highest value output of the system is not a report. It is a lane. Historical tape identifies obligors, supplier behavior, dilution, control quality, and recurring asset characteristics. Continuous monitoring preserves that knowledge as new assets arrive. Once that lane exists, capital can underwrite against something repeatable rather than anecdotal. Forward flow, warehouse lines, managed accounts, and syndication all depend on the same thing: a lane with known behavior and live controls.

[PLACEHOLDER FOR IMAGE: p27_capital_lanes.png]

5 to 10 active programs.

Sources: MINT origination funnel, lane analysis.

DISTRIBUTION

XIV. Standardization Precedes Securitization

Every scaled asset class standardized its data before it scaled its funding market.

Mortgages had MISMO. Commercial real estate had CREFC. Leveraged loans had LSTA. In every case, standardized data came before scaled funding. Trade receivables still lack a common schema, a common evidence format, and a common control taxonomy. That is why the asset class remains structurally bilateral and under securitized. The missing step is not more capital. It is a standard that capital can actually trust. MINT can become that standard by defining the checkpoint schema, evidence format, and control state a verified receivable must carry before it becomes programmable collateral.

[PLACEHOLDER FOR IMAGE: p28_standardization.png]

Sources: MISMO, CREFC, LSTA, trade finance standardization research.

XV. One Engine

One control architecture can verify many collateral types.

The insight is architectural, not sector specific. Receivables are simply the first market where the gap is acute and the data is already becoming machine readable. But the underlying engine, source capture, entity resolution, lien logic, remittance correlation, anomaly detection, and continuous monitoring, does not stop at invoices. The same control domains recur anywhere capital is financing cash flows against claimed assets. Once the engine exists, category expansion is not a new theory of the company. It is reuse of the same verification grammar in adjacent collateral systems.

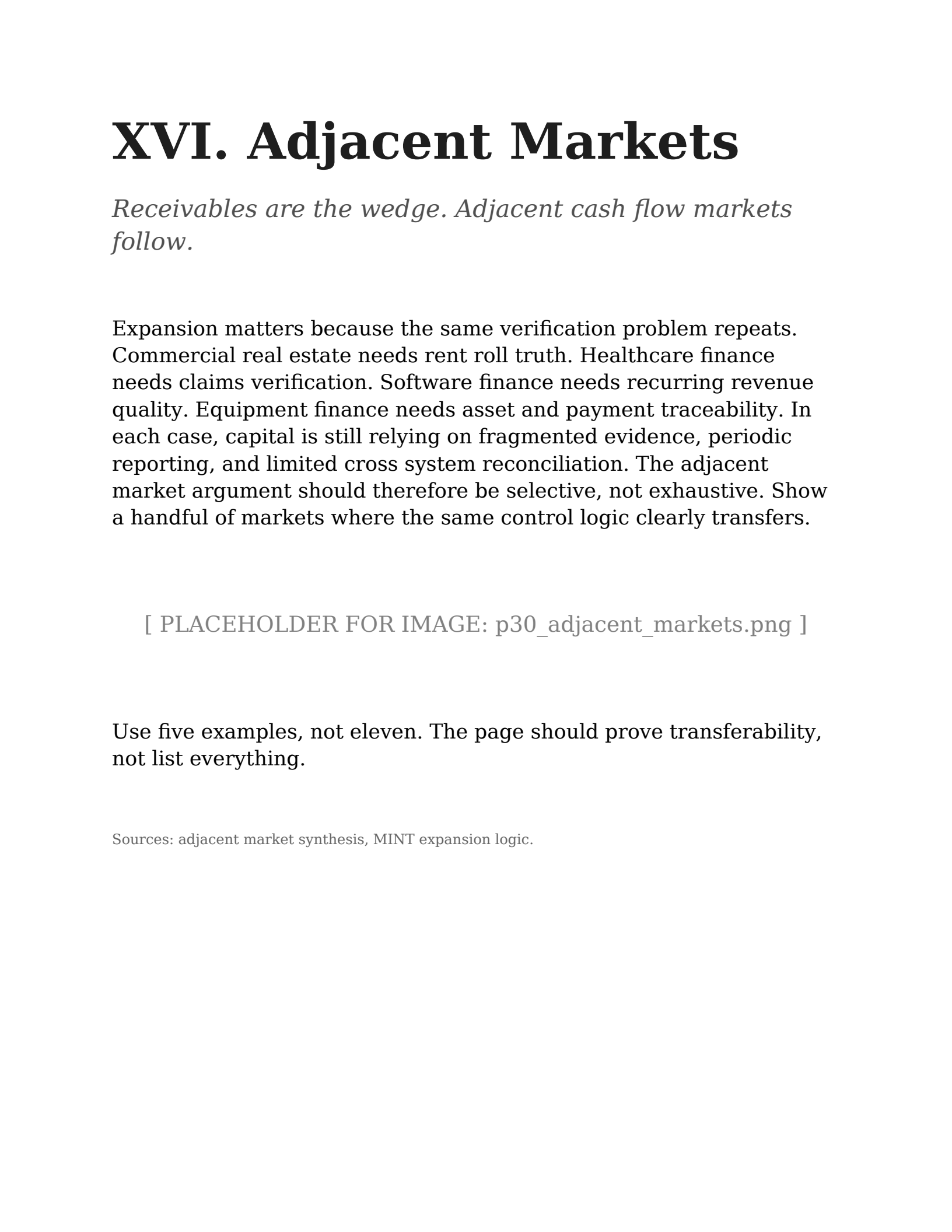
[PLACEHOLDER FOR IMAGE: p29_one_engine.png]

Sources: MINT architecture and adjacent market logic.

XVI. Adjacent Markets

Receivables are the wedge. Adjacent cash flow markets follow.

Expansion matters because the same verification problem repeats. Commercial real estate needs rent roll truth. Healthcare finance needs claims verification. Software finance needs recurring revenue quality. Equipment finance needs asset and payment traceability. In each case, capital is still relying on fragmented evidence, periodic reporting, and limited cross system reconciliation. The adjacent market argument should therefore be selective, not exhaustive. Show a handful of markets where the same control logic clearly transfers.



Use five examples, not eleven. The page should prove transferability, not list everything.

Sources: adjacent market synthesis, MINT expansion logic.

Conclusion

The company that defines the control state defines the market.

Fraud exposed the gap. Capital made the requirement explicit. Standards, payment rails, and enterprise execution made the solution technically possible. MINT resolves receivables into a control state, and that control state is what turns verification from cost center into market infrastructure. The supplier-side constraint is real but manageable. What changed is that supplier-side systems can now be enriched with sanctioned portal state, remittance evidence, public lien data, and machine-speed exception detection. The first product is receivables verification. The larger outcome is standard setting.

Once capital begins to price against a shared control state, the company that defines that state captures not just a workflow, but the market that forms around it.