Valid signature. Wrong payment state.

The security checks between a callback and a change to customer money.

DELIVERY CHECK

Signature verified

Business action: still to validate

A practical control pattern for cross-border payment platforms.

Two genuine events. One unsafe update.

ILLUSTRATIVE PAYOUT LIFECYCLE

01

COMPLETED arrives first

The system records the confirmed payout.

02

An older PROCESSING arrives

The handler blindly overwrites the status.

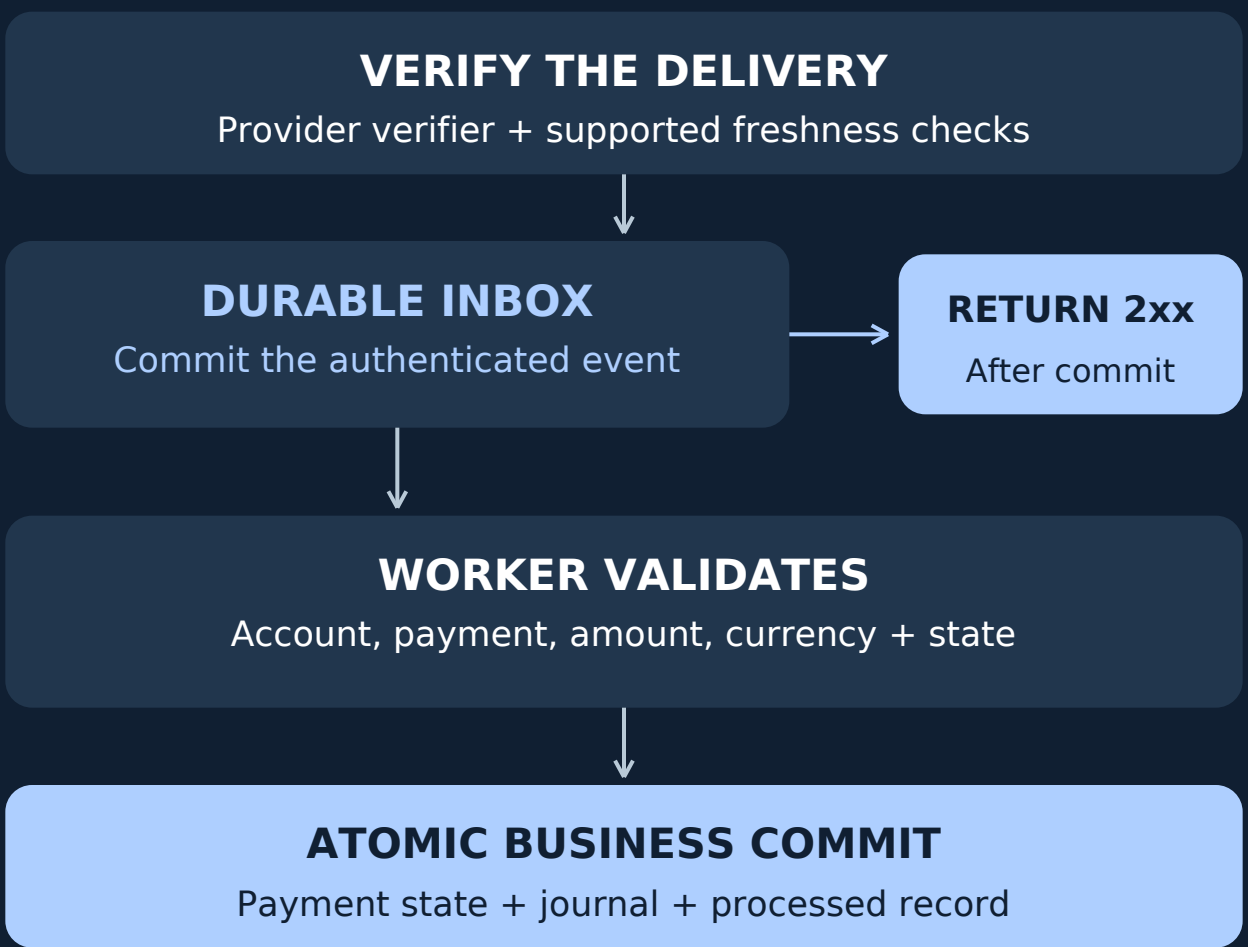
03

The dashboard goes backwards

Operations now sees an incorrect payment state.

A verified signature does not establish event order.

Verify. Persist. Then process.



Failed authentication: reject without financial writes.
A 2xx confirms durable receipt; processing may still be pending.

Use the provider's exact signing contract.

01 VERIFY THE SIGNED CONTENT

Use its maintained verifier and expected algorithm.
Stripe needs raw bytes; Adyen Standard signs selected fields.

02 CHECK FRESHNESS WHERE SUPPORTED

Enforce the authenticated delivery timestamp.
An old event and an old delivery signature are different.

03 PROTECT AND ROTATE SECRETS

Separate test and live secrets. Store them securely.
Test planned rotation; revoke compromised keys.

04 LIMIT THE PUBLIC ENDPOINT

Require HTTPS, limit request size and validate schema.
IP allowlisting is an extra layer, not identity proof.

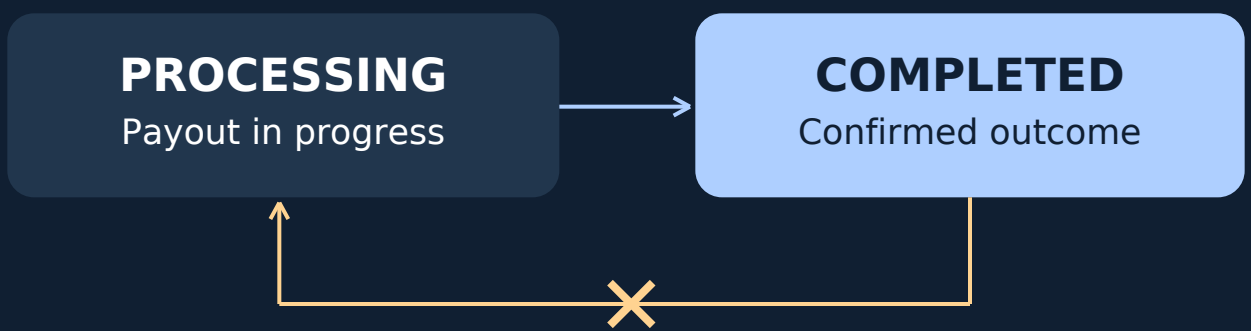
Does this event belong to this payment?

CHECK	MATCH THE STORED INSTRUCTION
Provider context	Expected provider, environment, merchant account and tenant.
Payment identity	Provider reference mapped to the exact internal payment attempt.
Economic details	Amount and currency for the same payment leg, using exact units.
Event meaning	Supported event type and its documented payment-state meaning.

Mismatch or missing evidence? Quarantine for review.
Resolve uncertain status through the trusted provider API.
Keep secrets and unnecessary payment data out of logs.

Model state changes. Keep corrections explicit.

SIMPLIFIED, PROVIDER-SPECIFIC STATE MODEL



An older PROCESSING event must not undo a confirmed COMPLETED state.

RETURNS AND REVERSALS

Model legitimate corrections as explicit transitions with linked correcting entries. Preserve the original journal.

Use documented sequence/version rules or retrieve current provider state. Arrival order alone cannot resolve conflicts.

Make the business effect idempotent.

Deduplicate delivery IDs. Also protect the business operation: separate events can describe the same effect.

ONE DATABASE TRANSACTION

01 Lock the payment; recheck the transition.

02 Enforce a unique constraint on the operation key.

03 Write the balanced journal entries.

04 Update state + mark the inbox event processed.

The key must identify the actual financial operation, including distinct refunds or reversals.
Separate ledger service? Use a durable outbox and an idempotent ledger API; one DB commit cannot span both.

Seven tests before the next release.

TEST	EXPECTED OUTCOME
Tampered signed data / invalid signature	Reject; zero financial writes.
Stale signed delivery timestamp	Reject per the provider's freshness protocol.
Wrong account, amount or currency	Quarantine and alert; no automatic update.
Two workers, same event	One financial effect; safe repeat handling.
Different IDs, same operation	Business-operation key blocks duplicate entries.
Older event arrives after completion	No prohibited state downgrade.
Crash around the DB commit	Resume safely; no lost or duplicate journal.

Also test secret rotation and alerting on stuck inbox events.

Can your ledger survive a genuine webhook delivered at the wrong time?

Bring engineering, security and payment operations into the same review.

Which control is hardest to implement consistently across your payout partners?

Brajkishor Pandey

linkedin.com/in/brajkishorpandey

PRIMARY TECHNICAL REFERENCES

Stripe | Webhooks: ordering and duplicate events
Adyen | Receive, store, acknowledge, process
Adyen | Provider-specific HMAC verification
OWASP | Webhook security
OWASP | Payment gateway integration