Money-bug checklist for code review

25 questions to ask on any pull request that touches refunds, payouts, ledgers or payment state.
Each targets a bug that can look correct in a diff. Pages 2–5 give a source, a test and a result line for each one.

REFUNDS

1 Can concurrent refunds exceed what was captured?
Two refunds can both pass a balance check. Enforce the cap atomically; bank-transfer refunds have no provider cap.

2 Is the refundable amount net of refunds and disputes?
Start from the captured amount, not the authorised one. A refund during an open dispute can pay the customer twice.

3 Does the refund account for every leg of a split payment?
Seller share, platform fee and tax each follow their own refund rule. Stripe, for one, keeps its original processing fee.

RETRIES, CRASHES AND IDEMPOTENCY

4 What if a call times out, or the process dies mid-way?
Both leave an unknown outcome. Record the intent first, then check status or retry with the same key.

5 Is the idempotency key created once per business intent?
Minted inside the retry loop, every attempt is new. Keyed on the order, a legitimate second refund is dropped.[1]

6 Can the same work run twice at once?
Requests race, queues redeliver, cron runs overlap and files get re-sent. Claim the work with a unique constraint.

7 Does the code retry only errors that are safe to retry?
Retry rate limits and timeouts with the same key. Never loop on hard declines: card networks charge for excess retries.

LEDGER AND BALANCES

8 Do debits and credits balance, in one transaction?
Balance each entry per currency and commit all legs at once, or a crash midway creates or destroys money.

9 Are balance checks atomic, and on the available balance?
Read-then-write lets two debits overdraw. Check available funds, net of holds, in the same step as the debit.

10 Are corrections posted as new reversing entries?
Editing or deleting a posted entry erases the audit trail and rewrites reports already sent.

STATE, DISPUTES AND WEBHOOKS

11 Is any state treated as final when it isn't?
A capture can be disputed months later, a refund can fail, a paid payout can bounce. Record each as a new event.

12 Are webhooks verified, de-duplicated and order-safe?
Check signatures, store event IDs to drop repeats, and act on current state: providers retry and reorder.

13 What finds and resolves payments stuck in pending?
Poll the provider, set a maximum age and alert past it. In India, a failed UPI transfer not reversed by T+1 costs ₹100 a day.[3]

AMOUNTS, CURRENCY AND ROUNDING

14 Are amounts exact: minor units or decimals, never floats?
`0.1 + 0.2` is `0.30000000000000004`. Use integer minor units or exact decimals; many JSON parsers read numbers as floats.

15 Are zero, negative, huge and at-limit amounts handled?
A negative amount can turn a charge into a credit. Paise in a 32-bit integer overflow near ₹2.1 crore. At the limit: `>` or `>=`?

16 Do amounts carry a currency, and conversions a rate?
JPY has 0 decimals, KWD 3: ×100 is not universal. Store each rate and its time, and decide which rate a refund uses.

17 Do splits (instalments, fees, tax) add up to the total?
₹1,000 in three ₹333.33 instalments collects ₹999.99. Assign the last paisa; pick per-line or per-invoice tax rounding.

RECONCILIATION AND TIME

18 Which timezone and cut-off define "today"?
00:30 IST is 19:00 UTC the day before. Limits, settlement and reports may use different days; map each one.

19 What happens on holidays, weekends and after cut-off?
NEFT settles on holidays; card settlement and provider payouts may not. Test a Friday evening before a long weekend.

20 Does the daily recon cover new fields, statuses and fees?
Anything this PR adds that recon doesn't know about drifts unnoticed. Match provider, bank and ledger; age the breaks.

CONTROLS AND ROLLOUT

21 Can this path move money without the usual checks?
Admin tools and scripts need the same authorisation, limits and screening. Manual credits need a second approver.

22 If this is wrong in production, what limits the damage?
Cap value per payment and per day, alert on odd volume, keep a kill switch. UCO Bank's IMPS error reached ₹820 crore.[2]

23 Is the rollout safe for money already in flight?
Old and new code run side by side. Handle statuses old code never saw, and stop backfills re-firing payouts.

AI-WRITTEN CODE

24 Did generated code invent a field or drop a guard?
Names the provider never sends; locks, keys and amount checks lost in a rewrite. Check the pinned API version.

25 Do the tests check intent, or only mirror the code?
Generated tests can assert whatever the code does. Watch for catch-all handlers that mark a failed call as done.

1 Stripe API reference, "Idempotent requests": in API v1, retries that reuse a key get the first request's saved response, `500` errors included, and keys can be pruned after 24 hours. API v2 retries failed work instead. docs.stripe.com/api/idempotent_requests

2 UCO Bank's disclosure, as reported on 16 Nov 2023: a technical issue in IMPS credited ₹820 crore to its customers over 10–13 Nov without the money arriving; 79% was recovered by blocking accounts. outlookbusiness.com

3 RBI circular DPSS.CO.PD No.629/02.01.014/2019-20 (20 Sept 2019). T is the calendar date; UPI transfers reverse by T+1, unconfirmed merchant payments by T+5. rbi.org.in

From **Vivek Yadav**, Ocean (getocean.dev). I'm studying how payments teams review money changes. Reply with what's missing.

SOURCES, TESTS AND RESULTS · QUESTIONS 1–7

Refunds, retries, crashes and idempotency

Sources are examples of documented behaviour, mostly from providers and regulators: check your own provider's and rail's rules. Each test turns one into a review case. Mark a result, and put notes or an evidence link in the box.

PR / CHANGE | REVIEWER | DATE

REFUNDS

1 Can concurrent refunds exceed what was captured?

☐ PASS ☐ FAIL ☐ N/A

Stripe rejects card refunds that total more than the charge. A refund you send as a separate payout or wallet credit has no such cap, and two of your own checks can both pass first. Stripe: Refund and cancel payments · PostgreSQL: Transaction isolation

TEST Fire two simultaneous refunds of 60 against a capture of 100. At most one may reserve funds.

NOTES

2 Is the refundable amount net of refunds and disputes?

☐ PASS ☐ FAIL ☐ N/A

An uncaptured payment can't be refunded, only cancelled. Stripe warns that a refund plus a bank-initiated dispute on a bank debit can give the customer two credits. Stripe: Refund and cancel payments · Stripe: How disputes work

TEST Authorise 100, capture 60, then refund 61: rejected. Open a dispute for 60, then refund: rejected or held.

NOTES

3 Does the refund account for every leg of a split payment?

☐ PASS ☐ FAIL ☐ N/A

Stripe doesn't return its processing fee. On destination charges the refund debits the platform; reverse the transfer to recover it from the seller. Stripe: Refund and cancel payments

TEST Trace seller, platform, fee and tax legs for a full and a partial refund against your agreed refund policy.

NOTES

RETRIES, CRASHES AND IDEMPOTENCY

4 What if a call times out, or the process dies mid-way?

☐ PASS ☐ FAIL ☐ N/A

Stripe allows same-key retries after network errors. The transactional outbox pattern stores the intent in the same transaction as the business change, so a relay can finish it. Stripe: Advanced error handling · microservices.io: Transactional outbox

TEST Kill the worker after the provider succeeds but before the ledger write. On restart: one refund, one ledger effect.

NOTES

5 Is the idempotency key created once per business intent?

☐ PASS ☐ FAIL ☐ N/A

In Stripe's API v1 a same-key retry replays the first saved response, and keys can be pruned after 24 hours. AWS separates a retry of one request from a new intent. Stripe: Idempotent requests · AWS: Making retries safe

TEST Restart the worker between attempts: the stored key is reused. Issue two partial refunds on one order: both succeed.

NOTES

6 Can the same work run twice at once?

☐ PASS ☐ FAIL ☐ N/A

PostgreSQL's INSERT … ON CONFLICT is atomic under concurrency. SQS standard queues can redeliver, and Kubernetes can start two Jobs for one scheduled time. PostgreSQL: INSERT / ON CONFLICT · AWS SQS: At-least-once delivery · Kubernetes: CronJob

TEST Race duplicate callers, redeliver after a crash, overlap two runs and ingest the same settlement file twice. Money moves once.

NOTES

7 Does the code retry only errors that are safe to retry?

☐ PASS ☐ FAIL ☐ N/A

Stripe separates content, network and server errors; a 500 may have had side effects. Visa's rules, as PayPal summarises them, bar reattempting some decline codes and add fees for excess retries. Stripe: Advanced error handling · PayPal: Avoid excessive-retry penalties

TEST Exercise a validation error, 429, timeout, 500, a soft decline and a hard decline. Confirm bounded backoff and no retry of the hard decline.

NOTES

Ledger, balances, state, disputes and webhooks

LEDGER AND BALANCES

8 Do debits and credits balance, in one transaction?

☐ PASS ☐ FAIL ☐ N/A

TigerBeetle guarantees equal debit and credit totals; linked events make several transfers succeed or fail together. TigerBeetle: Account guarantees · TigerBeetle: Linked events

TEST Fail the last leg of a multi-leg transfer. No partial entry may commit, and each currency must balance.

NOTES

9 Are balance checks atomic, and on the available balance?

☐ PASS ☐ FAIL ☐ N/A

TigerBeetle enforces balance limits atomically and reserves pending transfers apart from posted ones. Stripe refunds draw on the available balance, not pending amounts. TigerBeetle: Balance bounds · TigerBeetle: Two-phase transfers · Stripe: Refund and cancel payments

TEST Start at the limit and race two debits, one against funds still on hold. Compare the stored balance with the journal.

NOTES

10 Are corrections posted as new reversing entries?

☐ PASS ☐ FAIL ☐ N/A

TigerBeetle corrects a transfer by adding new transfers, never by editing or deleting the original, so history stays auditable. TigerBeetle: Correcting transfers

TEST Correct an amount, then correct the correction. Rebuild the history and final balance from entries alone.

NOTES

STATE, DISPUTES AND WEBHOOKS

11 Is any state treated as final when it isn't?

☐ PASS ☐ FAIL ☐ N/A

Stripe: card disputes typically arrive within 120 days, a refund can move to failed and return to your balance, and a paid payout can change to failed within 5 business days. Stripe: How disputes work · Stripe: Refund and cancel payments · Stripe: Payouts / payout failures

TEST Replay a dispute after a refund, a failed refund and a payout failure after paid. Each posts new entries; none rewrites history.

NOTES

12 Are webhooks verified, de-duplicated and order-safe?

☐ PASS ☐ FAIL ☐ N/A

Stripe requires signature checks and warns that events can arrive duplicated and out of order. Stripe: Receive events / best practices

TEST Send a bad signature, a duplicate event ID and reversed event order. Only valid money effects may occur.

NOTES

13 What finds and resolves payments stuck in pending?

☐ PASS ☐ FAIL ☐ N/A

RBI: a UPI transfer debited but not credited is reversed by T+1; a merchant payment without confirmation by T+5. T is the calendar date; ₹100/day compensation after. RBI: Failed-transaction circular, 20 Sept 2019

TEST Lose a webhook, then recover by status poll inside the calendar-day deadline. Past the maximum age, someone is alerted.

NOTES

Amounts, currency, reconciliation and time

AMOUNTS, CURRENCY AND ROUNDING

14 Are amounts exact: minor units or decimals, never floats?

☐ PASS ☐ FAIL ☐ N/A

PostgreSQL's numeric is exact; real and double precision are not. JSON numbers are often parsed as doubles, so large values can lose precision in transit. PostgreSQL: Numeric types · RFC 8259 §6: Numbers

TEST Test rates, fractional allocations and the largest amount you accept. Define the rounding of the final unit.

NOTES

15 Are zero, negative, huge and at-limit amounts handled?

☐ PASS ☐ FAIL ☐ N/A

PostgreSQL's integer type tops out at 2,147,483,647: about ₹2.14 crore in paise. Stripe caps amounts by digit count, which varies by currency and network. PostgreSQL: Numeric types · Stripe: Supported currencies

TEST Send 0, −1, the maximum plus one, and amounts just below, at and above each limit. Each is rejected or handled on purpose.

NOTES

16 Do amounts carry a currency, and conversions a rate?

☐ PASS ☐ FAIL ☐ N/A

ISO exponents differ: JPY 0, KWD 3, BHD 3. Stripe's example: a 100 EUR sale disputed three months later cost the seller 107.86 EUR because the rate had moved. Worldpay: Currency codes and exponents · Stripe: How disputes work

TEST Round-trip one unit of each currency. Refund a converted payment after the rate moves; check who absorbs the difference.

NOTES

17 Do splits (instalments, fees, tax) add up to the total?

☐ PASS ☐ FAIL ☐ N/A

Adyen documents half-to-even rounding for automatic splits. Whatever the rule, the parts must sum to the whole. Adyen: Split payments automatically

TEST Split ₹1,000 three ways and find the leftover paisa, then partially refund the split. Compare per-line and per-invoice tax.

NOTES

RECONCILIATION AND TIME

18 Which timezone and cut-off define "today"?

☐ PASS ☐ FAIL ☐ N/A

Stripe report ranges follow the account's timezone or UTC, and the day boundary changes which records are included. Stripe: Report configuration

TEST Test both sides of midnight and of each cut-off, plus daylight-saving changes where they apply.

NOTES

19 What happens on holidays, weekends and after cut-off?

☐ PASS ☐ FAIL ☐ N/A

RBI made NEFT available on all days of the year, holidays included, from 16 Dec 2019. Adyen documents cut-offs and bank-holiday payout delays. RBI: NEFT on a 24×7 basis, 6 Dec 2019 · Adyen: Getting paid · Adyen: Sales day payout

TEST Pay before and after cut-off on the Friday before a long weekend. Check the expected settlement date on each rail.

NOTES

20 Does the daily recon cover new fields, statuses and fees?

☐ PASS ☐ FAIL ☐ N/A

Stripe's payout reconciliation report covers payments, refunds, disputes and fees; what it supports depends on payout type. Stripe: Payout reconciliation report

TEST Add a fee or status, omit a row and flip a sign. Recon must flag each one, and an unmatched item must have an owner.

NOTES

Controls, rollout and AI-written code

CONTROLS AND ROLLOUT

21 Can this path move money without the usual checks?

☐ PASS ☐ FAIL ☐ N/A

OWASP ranks broken object-level and function-level authorisation among the top API risks, and says logs must exclude bank account and card holder data. OWASP API1:2023 Broken object-level authorization · OWASP API5:2023 Broken function-level authorization · OWASP: Logging cheat sheet

TEST Call the new path as another tenant, as a non-admin and above the limit. Check no card or bank data reaches the logs.

NOTES

22 If this is wrong in production, what limits the damage?

☐ PASS ☐ FAIL ☐ N/A

UCO Bank said a technical issue in IMPS credited ₹820 crore to its customers over 10–13 Nov 2023 without the money arriving. It recovered 79% by blocking accounts. Outlook Business: UCO Bank IMPS credits, 16 Nov 2023

TEST Run it with a wrong amount in staging. Find which cap, alert or switch stops it, and how many payments get through first.

NOTES

23 Is the rollout safe for money already in flight?

☐ PASS ☐ FAIL ☐ N/A

SEC: Knight Capital deployed new code incorrectly to a router that still held an unused, defective function. It sent over 4 million orders in 45 minutes and lost more than $460 million. SEC: Knight Capital order, 16 Oct 2013

TEST Deploy to half the workers, process in-flight payments on both versions, then roll back. Dry-run every backfill with money movement off.

NOTES

AI-WRITTEN CODE

24 Did generated code invent a field or drop a guard?

☐ PASS ☐ FAIL ☐ N/A

GitHub warns generated code can look valid yet be wrong. Stripe event shapes depend on the configured API version. GitHub: Responsible use of inline suggestions · Stripe: Receive events / best practices

TEST Check each new field, status and error code against real response fixtures. List every lock, key and amount check before and after.

NOTES

25 Do the tests check intent, or only mirror the code?

☐ PASS ☐ FAIL ☐ N/A

GitHub recommends reviewing and testing generated code. This is a review method, not a measured failure rate. GitHub: Responsible use of inline suggestions

TEST Break a guard on purpose: a test must fail. Make the provider mock time out and return 500; nothing may be marked successful.

NOTES

NOT COVERED ABOVE

Recurring billing and mandates; batch files and their control totals; value date against booking date, and period close; interest and day-count rules in lending; card-scheme and rail rulebooks.

NOTES