

D07 退款与对账域 · 设计文档

本域总览见《账号计费中心 · 结构大纲》。本文为该域完整设计：定位与边界 / 角色与依赖 / 数据模型 / 核心流程 / 接口契约 / 关键约束与验收标准。

排序说明：先数据模型（事实结构）→ 再核心流程（结构之上的运行路径）→ 最后接口契约（流程的对外投影）。

1. 定位与边界

定位：资金流出的唯一闸门与资损防线的最后一道。回答三个问题——「这笔钱该不该退、由谁批准」（审批链与二审门禁）、「钱到底出去了多少钱」（以渠道实退为准的冲销口径）、「账实是否相符」（渠道账单与本地流水的双向对账）。

核心概念

概念	承载	语义
退款申请	<code>customer_orders</code> 的 <code>refunding</code> 状态	申请只改状态不动钱；申请人不等于审批人
本次定额	<code>customer_orders.refund_amount</code>	审批时定格，重试与人工收敛沿用；后续不得超原额
累计已退	<code>customer_orders.refunded_amount</code>	部分与多次退款的唯一计数器，出款成功才累计
剩余可退	派生量 <code>refundable_of</code>	订单金额 - 累计已退，是每单上限而非全局常量
退款请求号	<code>customer_orders.refund_request_no</code>	渠道幂等键（订单号加序号），同号只退一次
冲销流水	<code>customer_transactions</code> 的 <code>refund</code> 类型行	只增反转行，金额为负；账务真相源
对账差异	<code>risk_events</code> 台账（属风控域）	本域产生与收敛，台账归风控域
待线下打款	<code>customer_orders.offline_paid_confirmed_at</code>	纯台账语义，不动账、不改状态

关键口径

- 金额口径：一律元、6 位小数、字符串传输。退款定额经门禁恒为等效 2 位小数，渠道回执亦为 2 位，故比对按分精确比较、不设容差。
- 出款以渠道为准：只有渠道确认出款成功才冲销本地账；渠道失败或结果未知时一分钱都不动。
- 不确定即不收敛：渠道报成功但无法核实单笔实退金额时，保持处理中并把结果存疑交人工，绝不以本地定额自证冲销。
- 仅现金通道：可退订单限于充值类型，退款回的是现金、不恢复赠金，杜绝「堆赠金 → 现金套利」。
- 清偿后退款：退款把现金推为负是正常态，负债回潮由欠费标记的单一重算规则自然处理，不另设拒绝条件。
- 对账锚点是本地流水：以本地退款流水为基准逐笔对齐渠道账单行，不以账单为主反查本地。

边界

- 不管钱包记账原语：现金增减、流水写入、欠费标记重算都在钱包与账务域；本域只发起冲销。

- 不管订单状态机本体与渠道凭据：下单、支付回调、凭据配置在订购与支付域；本域消费其订单行与渠道能力。
- 不管用量对账与通知投递：用量对账属计量与计费域，触达通道与模板在通知与触达域。
- 不管台账本体与运营面权限载体：台账定义、规则配置与处置台在风控与合规域；运营端点的统一索引与平台员工权限登记在运营管理域。

归属口径

- 门户自助申请的频控在本域，与审批侧二审门禁正交；对账差异的产生与收敛在本域，台账行结构属风控与合规域。

2. 角色与依赖

能力矩阵

能力	门户用户	运营面	计费路由 (router)	数据面网关
自助申请退款	✓ (本人订单)	✓ (代客申请)	✗	✗
审批通过 / 驳回	✗	✓ (实人门禁)	✗	✗
二审登记 / 复审	✗	✓ (须不同操作人)	✗	✗
重试 / 人工结清 / 放弃 / 线下确认	✗	✓	✗	✗
触发轮询与渠道对账	✗	✗	✗	✗ (部署侧定时与进程内扫描触发)

- 出款类端点（审批通过、人工结清、放弃、重试、线下确认）走运营面实人门禁，操作人须是在册、在用的平台员工。
- 申请与驳回不动钱，故不设实人门禁；但操作人线索不得静默缺失：缺操作人时审计落来源通道标记，提供了但非标识格式则显式拒绝而不降级为空值。

上游依赖

上游	依赖内容	语义
订购与支付域	订单行、状态与 <code>paid_at</code> 、渠道、支付时点	可退订单来源；只退已支付、未退尽的充值单
钱包与账务域	现金余额、只增流水、欠费标记重算	冲销的落账目标；余额为负是正常态
外部资金通道	退款接口、单笔退款查询、日账单	出款真相与对账账单一侧
运营管理域	平台员工与权限范围	出款资格与四眼原则的身份真相

下游被引用

引用方	引用内容	语义
风控与合规域	退款异常与渠道差异信号	落处置台账并分级处置
通知与触达域	到账 / 失败 / 线下打款文案	成功与失败触达的投递
账户状态与准入域	冲销后的余额变更事件	退款是解封路径，须即时发布状态
订购与支付域	退款进度状态与归一原因码	订单列表与详情展示「部分已退 / 待二审」标记

3. 数据模型

本域无自有表：退款以订单行的退款相关列与资金流水的退款类型行承载，对账差异落风控处置台账。

3.1 域内关联总览

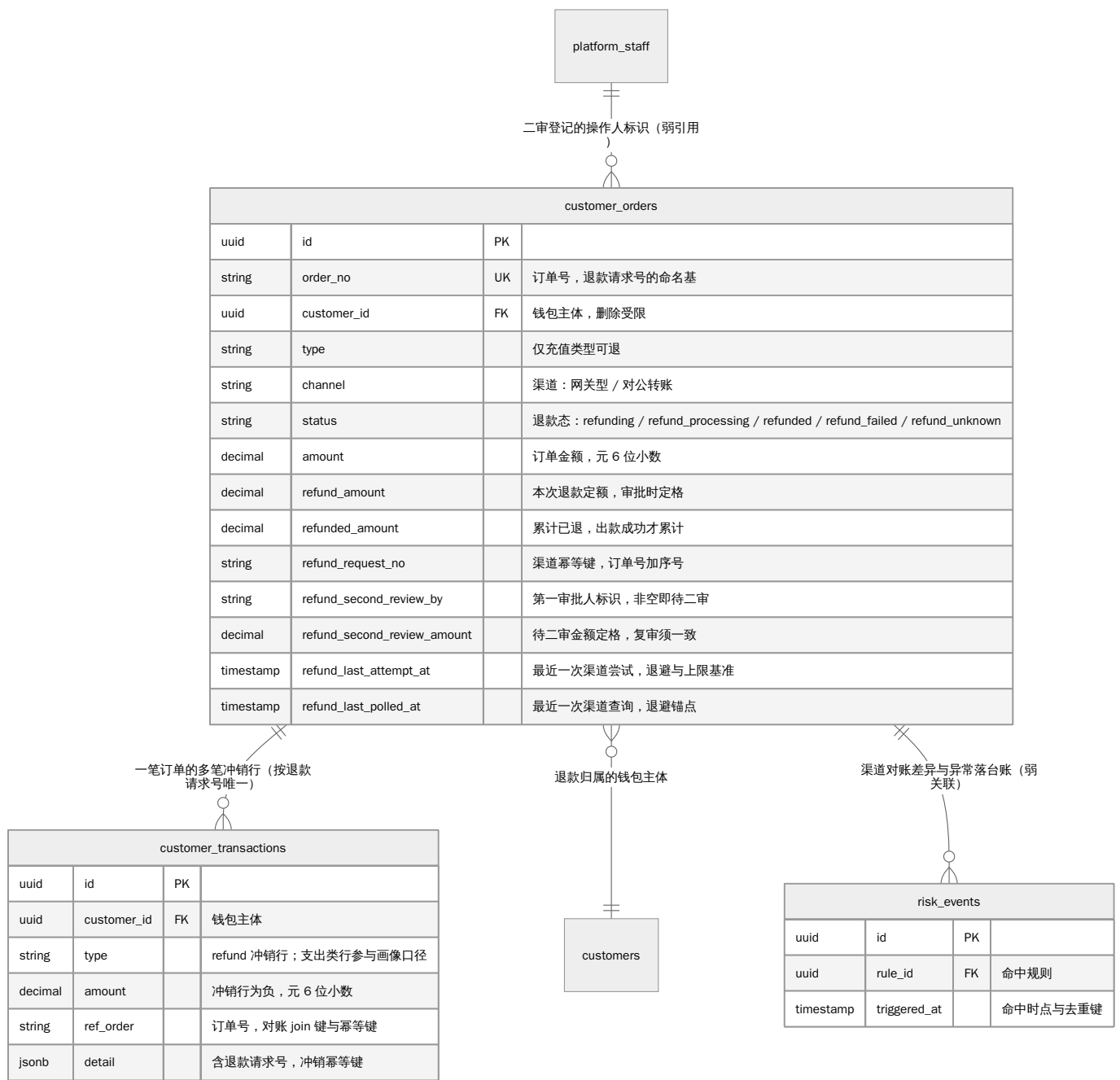


图 1

退款请求号落流水明细而非独立表：冲销行的唯一索引以「订单号 + 明细中的退款请求号」为键，部分索引收窄到退款类型，历史无该键的行天然不受影响。

3.2 域间引用

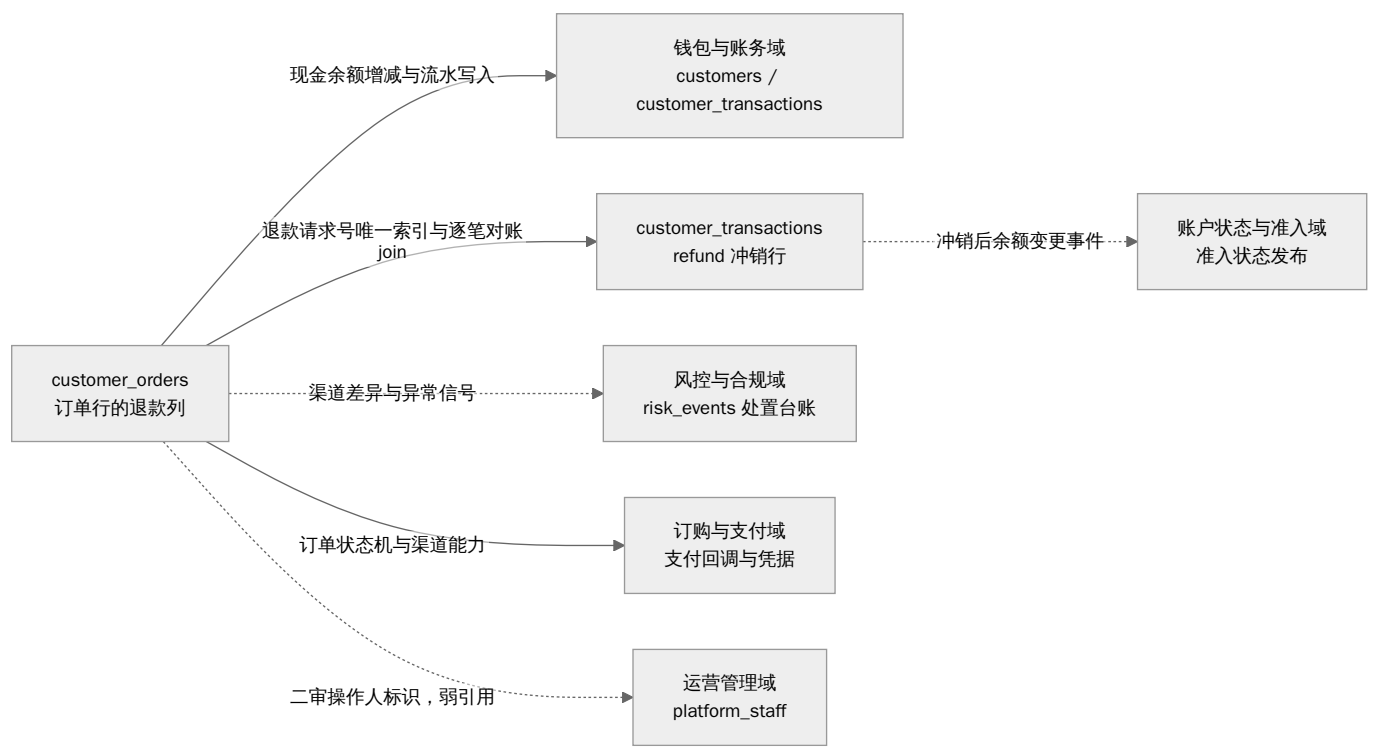


图 2

- 订单行的退款列与流水、台账之间不建跨表外键：流水以订单号弱引用、台账以订单为弱关联，避免写路径被删除约束拖住；台账行结构属风控域，本域只写「差异已产生」这一事实与收敛动作。

3.3 表清单

表	读写	关键字段
customer_order_s	读写	order_no / customer_id / type / channel / status / amount / refund_amount / refunded_amount / refund_request_no / refund_failed_reason / refund_second_review_by / refund_second_review_amount / refund_last_attempt_at / offline_paid_confirmed_at
customer_r_transactions	写 (只增) + 读	customer_id / type / amount / ref_order / detail / created_at
customers	只读	cash_balance (画像与推负判定) / overdue_since (派生标记, 不作债务判据)
operation_logs	读 (频控计数) + 写 (留痕)	actor_id / action / target_id / created_at / detail
risk_events	写 (差异与异常落台账)	rule_id / customer_id / organization_id / status / triggered_at

表	读写	关键字段
platfor m_staff	只读	user_id / status / scopes (出款资格)

3.4 设计约束

- 1. 冲销幂等唯一：部分唯一索引按「订单号 + 明细中的退款请求号」建立、仅覆盖退款类型行；同订单同请求号至多一行冲销流水，并发撞索引即收敛为幂等返回。
 - 2. 流水只增：冲销一律新增反转行，数据库层拒绝改写与删除既有流水；已出款的退款只能靠新增调整行更正。
 - 3. 金额精度：退款定额与渠道比对口径均为元、2 位小数等效值；订单金额列宽 20 位，入参越界在入口即拒。
 - 4. 累计口径唯一：累计已退只由出款成功路径累加，失败与未知路径不触碰该列，部分退款的可退额度不被虚高或挤压。
 - 5. 待二审定格非空即门禁：待二审人标识与定格金额同生命周期，出款、驳回、放弃、新一轮发起四处一并清空；带标记的订单只接受「同金额 + 不同操作人」复审。
 - 6. 状态取值封闭：退款相关状态仅取 `refunding` / `refund_processing` / `refunded` / `refund_failed` / `refund_unknown` 五值，状态列宽须容纳最长值；部分退款完成后回 `paid`，故不得用订单终态判退款幂等，幂等一律以退款请求号为准。
-

4. 核心流程

4.1 申请与审批主线

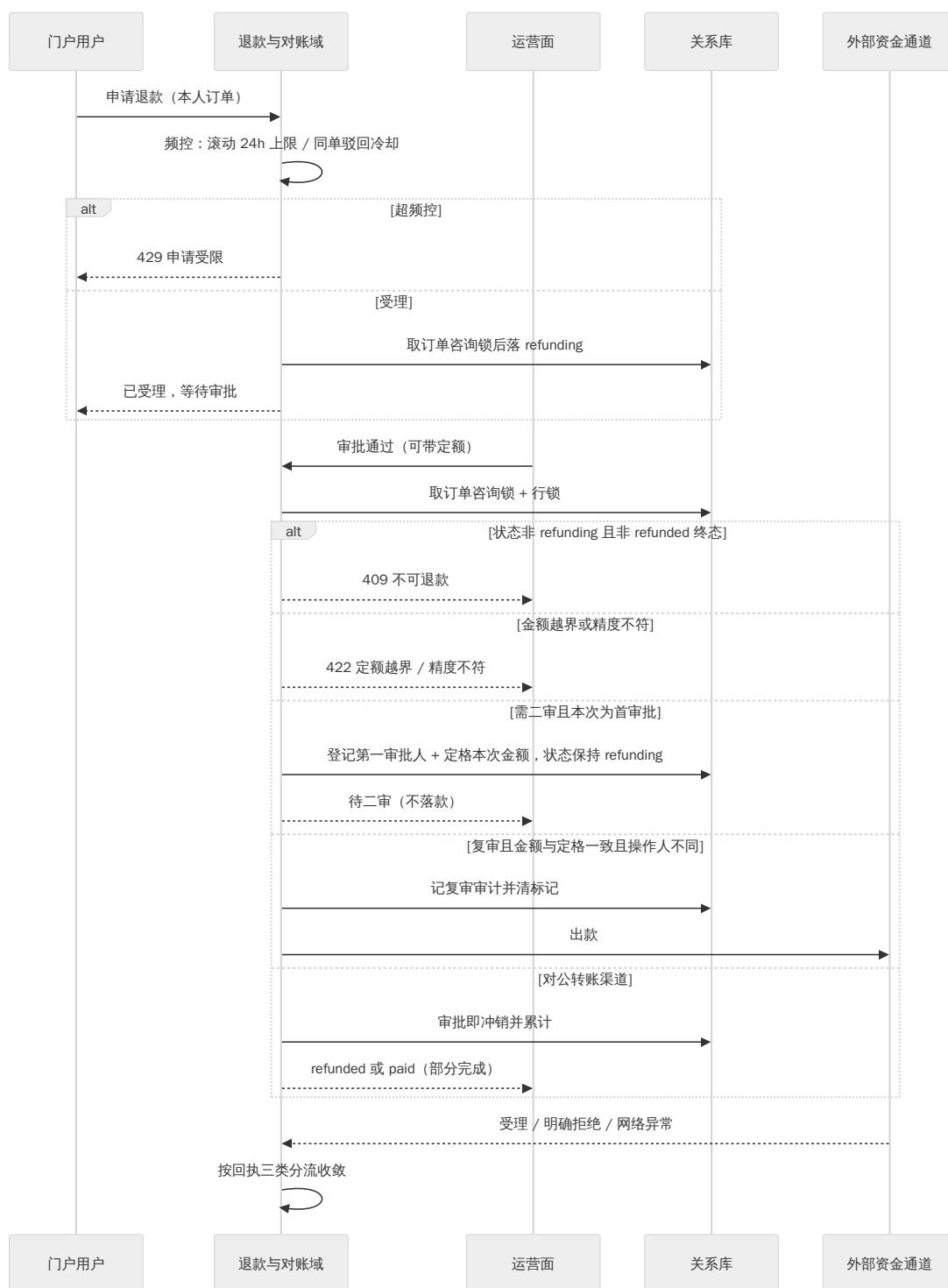


图 3

- 审批定额缺省为剩余可退全额；门禁为「大于 0 且不超过剩余可退」外加等效 2 位小数校验，违规即拒，不静默取整。
- 出款按渠道分派：网关型渠道走两阶段（先落处理中并提交、再锁外调渠道）；对公转账不调渠道，审批即冲销。

4.2 二审门禁与金额定格

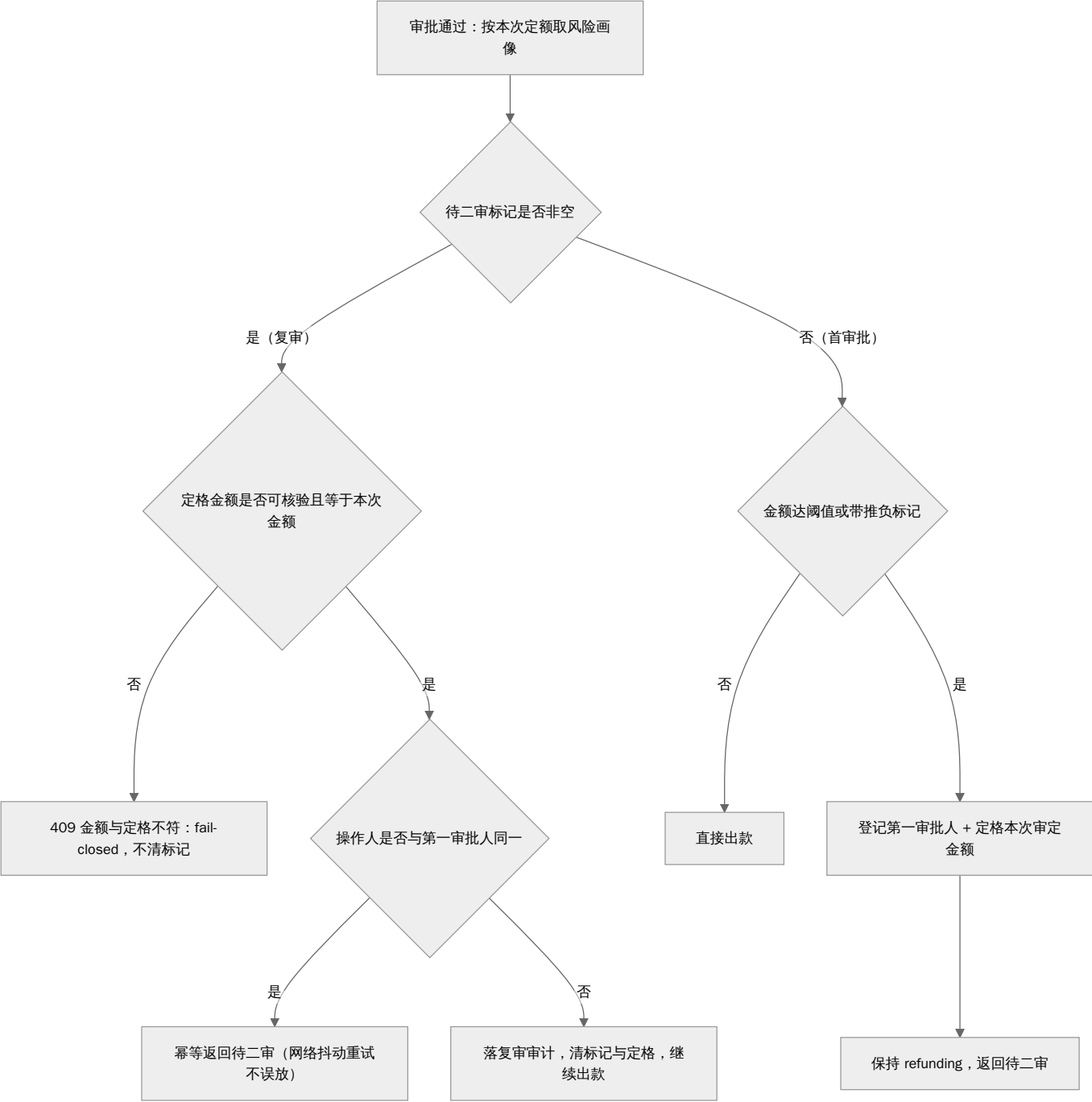


图 4

- 判定为「金额达阈值」或「退款将把现金推为负」之一即需不同操作人二次审批；推负一档可单独关闭，阈值一档为 0 即关闭。
- 定格是四眼原则的支点：不钉金额则第二审批人可换任意金额绕过，画像按新金额重算而第一审批人从未见过该金额。复审不符一律拒绝且不清标记——绕过者不能顺手清掉标记再重来，只能驳回后重新发起。
- 存量待审行无定格金额可核验时按「不可核验即拒」处理：猜一个金额写进去更危险。

4.3 审批前风险画像（只读，不持锁）

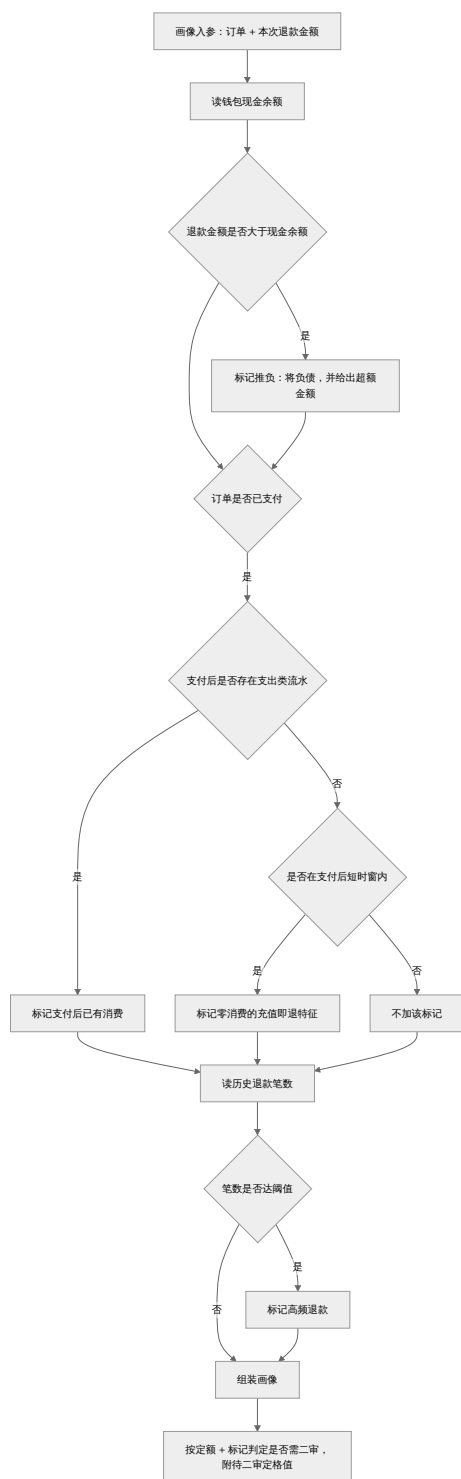


图 5

- 读出四类事实（现金余额 / 剩余可退 / 本次金额 / 历史退款笔数）、四个归一标记与二审判定，以及待二审时的第一审批人与定格金额（供弹窗预填，否则必然复审失败）。
- 支出类流水口径为全计：用量扣费、余额转让、负向调整都算消费——「充值 → 转账 → 退款」与「充值即退」同为套利变体；赠金抵扣行同样计入，它代表已发生用量。
- 不持锁的理由：画像只读、只呈现、不决策，且在审批入口内于订单锁之后调用；推负判定以出款时点的真实扣回为准（扣回无余额谓词、可为负），画像偏差不放过资损。若画像持锁，弹窗读与出款串行化。

4.4 部分与多次退款

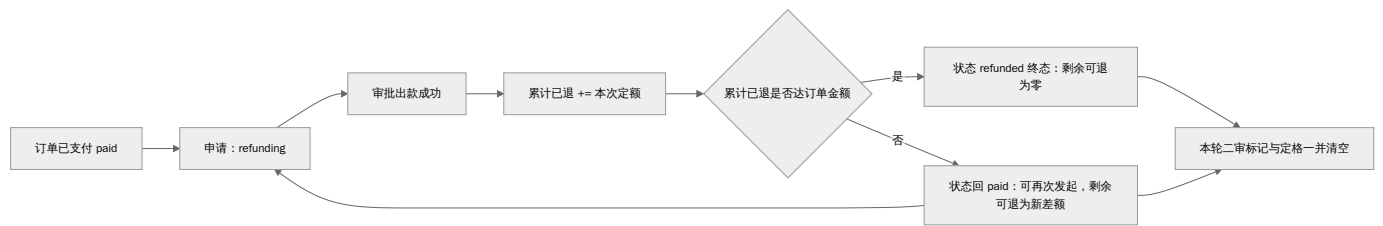


图 6

- 剩余可退 = 订单金额 - 累计已退，是每单上限，申请与审批两道都按此判定，额度退尽即拒。
- 并发串行化是双保险：应用层为「订单咨询锁 + 行锁」的锁域，同订单各退款收敛入口共用；数据库层为「订单号 + 退款请求号」的部分唯一索引，后到者撞索引即收敛为幂等返回。
- 冲销幂等不能靠订单终态：部分退款后订单回已支付态，反而是「看起来可再退」的正常态；幂等键是与渠道共享的退款请求号，它在审批锁内按「已有退款冲销行数 + 1」推导，串行无竞态，重试与人工结清沿用当次号。

4.5 渠道出款三阶段与实退金额比对

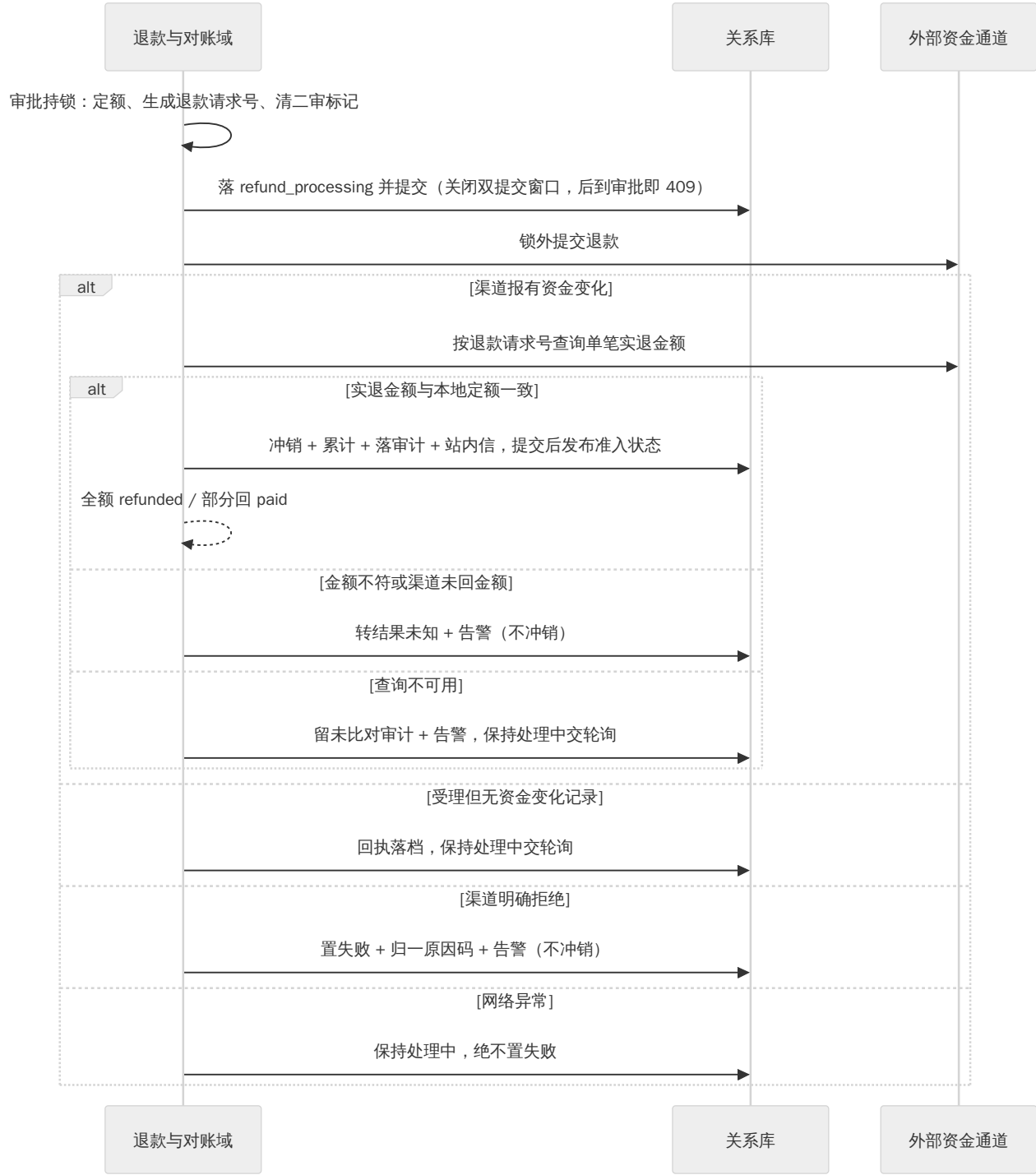


图 7

- 渠道实退为准：渠道报「有资金变化」只证明本次请求有过资金动作，不证明实退额等于本地定额——部分退、超额退、后台人工操作都会让两者背离，故必须另查单笔明细按 2 位小数精确比对。
- 冲销写法：另写一条退款类型反转行，金额为负、余额快照为冲销后余额（可为负），同事务重算欠费标记并发布准入状态；回执原文与交易号落订单行但不下发门户。

4.6 异常三分支收敛

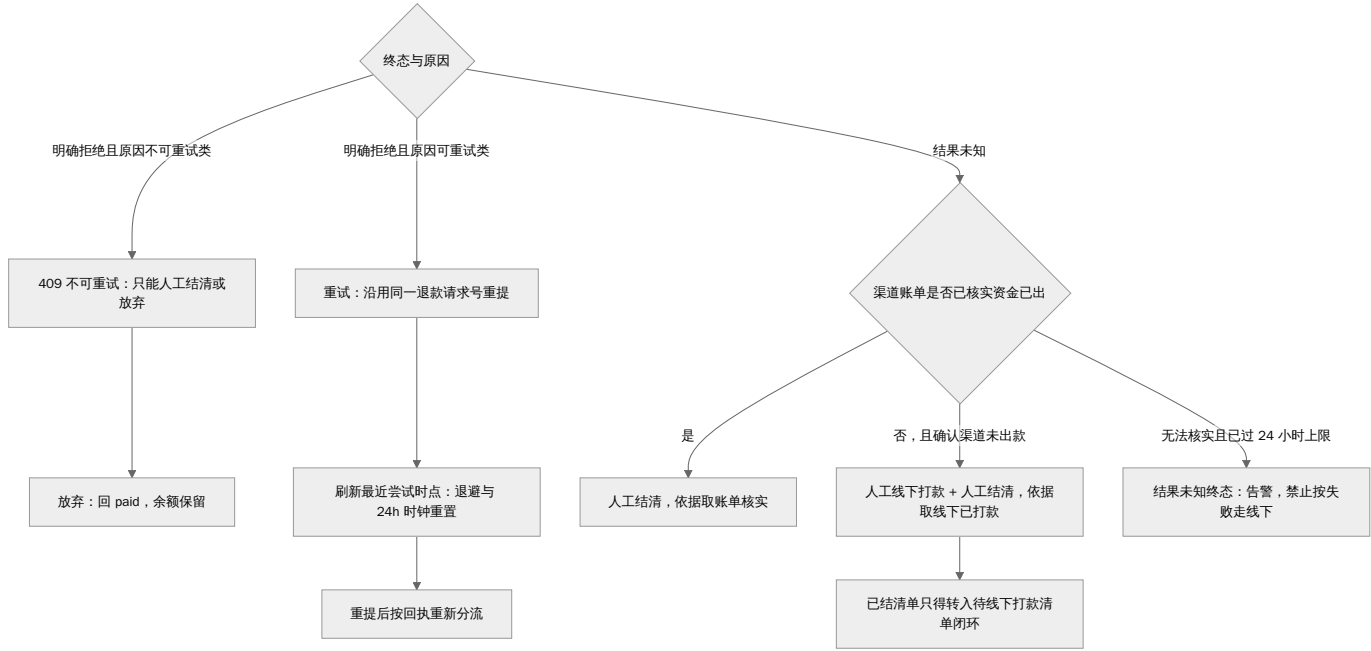


图 8

- 两类终态语义必须分清：失败 = 渠道明确未出款，可放弃回已支付态（余额保留）；未知 = 资金可能已出账，按失败走线下打款即渠道退一次、线下再退一次的双重退款，故未知只接受「渠道账单核实已退」这一种结清依据。
- 终止（放弃）也有禁用类：某些失败原因意味着「可能已退过」，回退会让余额保留与渠道已退款双得。
- 结果未知的 24 小时上限自最近一次渠道尝试起算，每次重试即重置时钟。

4.7 轮询收敛与退避

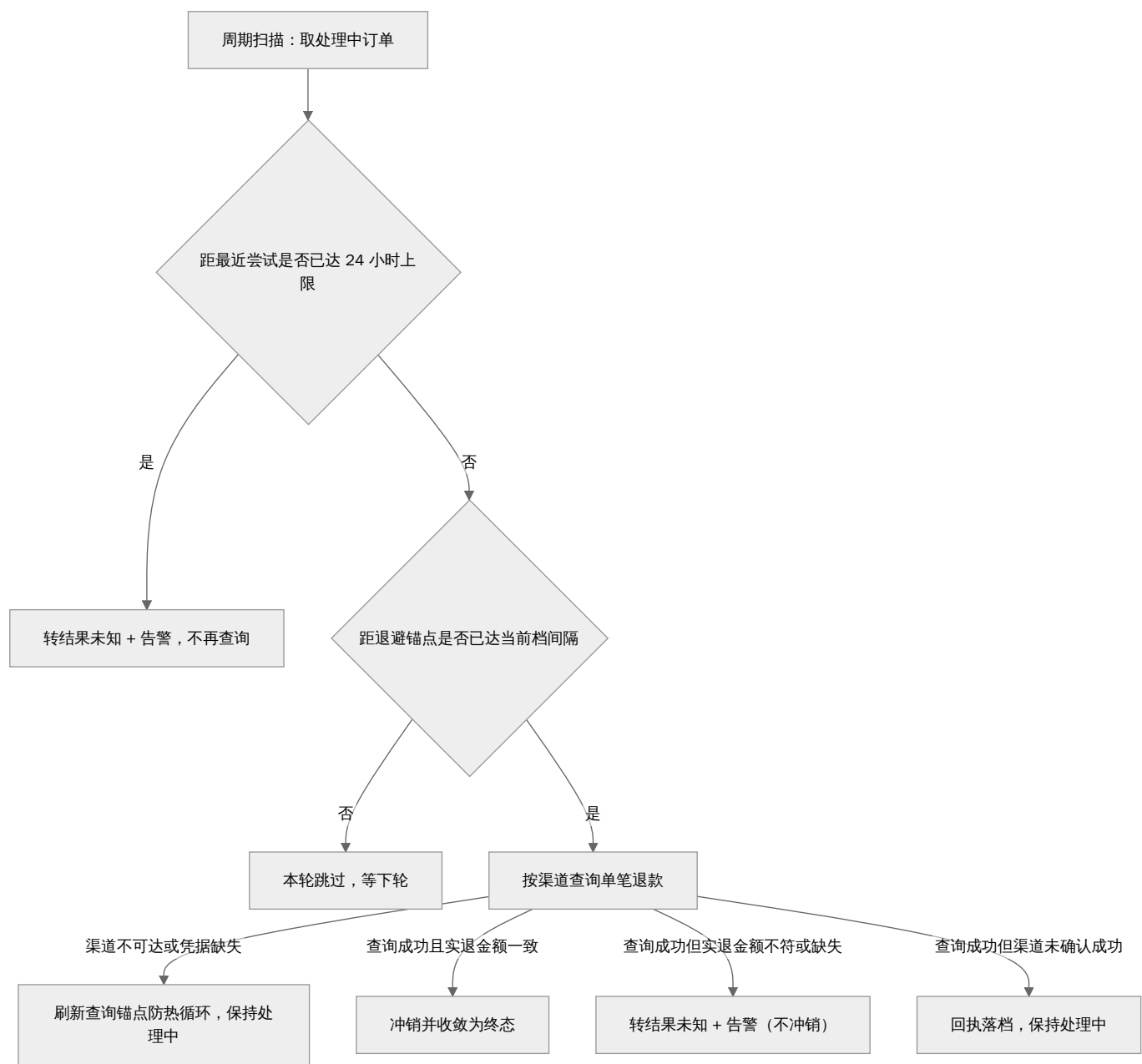


图 9

- 退避档按自渠道提交起的账龄升档（分钟级到小时级），间隔锚点为上次查询时点、无记录时以提交时点为锚——机会式扫描下若无锚点，首查时点可能被永久跳过。
- 每单独立短会话，单笔异常只记日志不拖垮整轮；收敛入口各自加锁且幂等，多副本与手动触发并发安全；结果未知的判定在锁内复检到期条件，旧判定不直接落终态。

4.8 线下打款与待核对清单

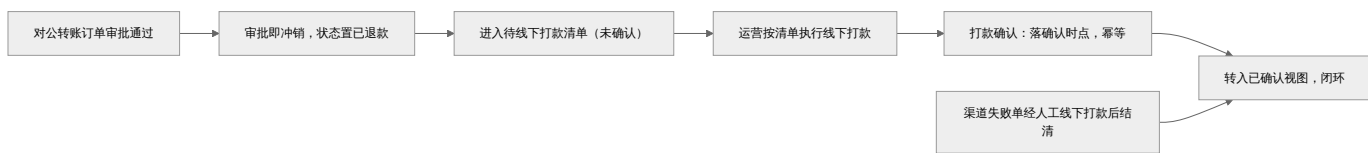


图 10

- 线下确认纯台账语义：不写流水、不动余额、不改状态，只落确认时点与审计；与「人工结清」作用对象不同，二者不重叠。

4.9 渠道退款对账与差异分类

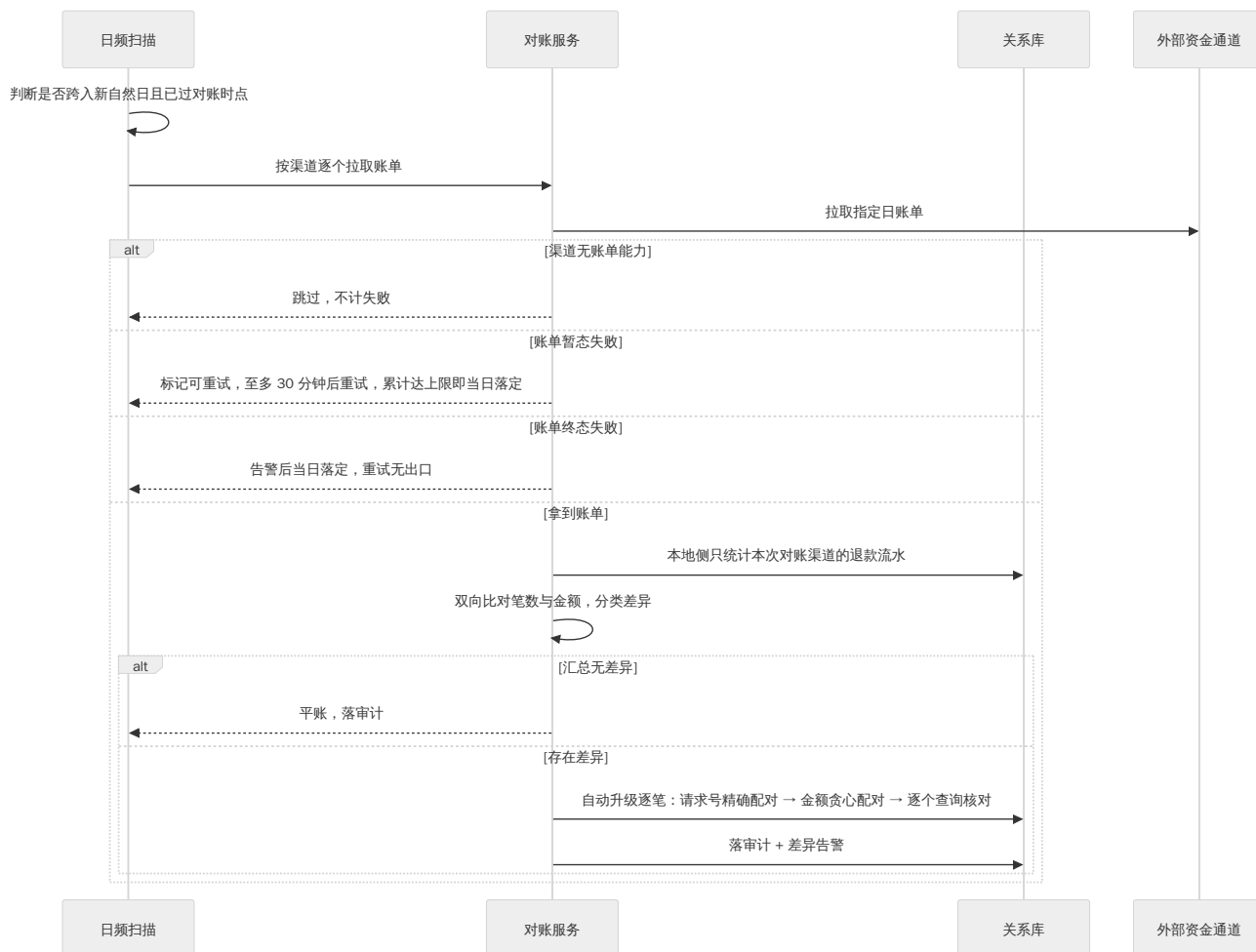


图 11

- 两层结构：汇总级比对「本地该渠道退款笔数与金额」对「账单退款行汇总」；汇总有差异（或强制逐笔）时自动升级逐笔，省去无差异日的明细成本。
- 锚点是本地流水：逐笔对齐以本地退款流水为基准匹配账单行，配对键优先退款请求号；本地侧排序键为「时点 + 请求号」，保证同单多笔同额下配对稳定、同日重跑一致（幂等）。
- 双向比对与差异分类：两侧键集合取并集，任一侧缺失或两侧笔数/金额不等都出差异；金额取绝对值后按 2 位小数精确比较、无容差。分类四类——本地独有（含孤儿子类）、账单独有、两侧皆有但金额或笔数不符、被渠道查询确认的「账单缺行」标记。
- 渠道过滤口径：本地侧必须按本次对账的渠道过滤（账单一次只拉一个渠道）；若按全集过滤，另一渠道的退款会在本轮全部落成假差异，真实差异被假告警淹没。孤儿行不受该过滤影响，也不得静默消失。
- 「账单缺行但渠道确认已退」是资金已出、账实已平、只是账单口径缺行的情形，须单列标记供人工分流；差异落审计与告警，台账结构属风控与合规域，本域只产生事实并收敛可收敛项。

5. 接口契约

5.1 门户自助 (/api/account)

方法	路径	语义
POST	/api/account/orders/{order_no}/refund-apply	客户自助退款申请：本人已支付充值订单 → 待审批；跨用户订单按订单不存在处理；滚动 24h 上限超限与同单驳回冷却内分别拒绝；期望金额仅审计参考

- 申请不设实人门禁（不动钱），操作人恒为客户本人；退款进度与归一原因码的读侧展示与订单列表同源共用（详见订购与支付域）。

5.2 内部退款与对账 (/internal)

方法	路径	语义
POST	/internal/orders/{order_no}/refund-request	运营侧发起退款申请（对账冲正 / 代客申请）
POST	/internal/orders/{order_no}/refund-approve	审批通过：金额定额 + 二审门禁 + 渠道出款；返回已退款 / 回已支付 / 处理中 / 失败
POST	/internal/orders/{order_no}/refund-reject	审批驳回：待审批 → 已支付，无冲销
POST	/internal/orders/refunds/poll	退款轮询（幂等）：扫处理中到点单查渠道收敛；供部署侧定时与手动兜底
POST	/internal/orders/refunds/reconcile-channel	渠道退款对账（汇总级 + 逐笔，幂等）：指定账单日、模式与渠道；供手动补跑
GET	/internal/orders/refunds/offline-pending	待线下打款核对清单：对公转账已退款单，可按已确认过滤

- 审批出款端点须运营范围令牌，且另要求操作人为在册、在用、持有出款权限的平台员工，否则统一按无权限拒绝且不区分原因。
- 对账端点的账单日、模式与渠道为受约束取值（仅汇总 / 强制逐笔 / 有差异自动升级）；轮询与对账均幂等。

5.3 运营面退款处置 (/api/account/ops)

方法	路径	语义
POST	/api/account/ops/orders/{order_no}/refund-request	运营发起退款（实人令牌，操作人恒为令牌本人）
POST	/api/account/ops/orders/{order_no}/refund-approve	审批通过（同 5.2 语义）
POST	/api/account/ops/orders/{order_no}/refund-reject	审批驳回
POST	/api/account/ops/orders/{order_no}/refund-retry	同号重提；不可重试类拒绝
POST	/api/account/ops/orders/{order_no}/refund-manual-settle	人工结清：依据与状态强绑定；幂等

方法	路径	语义
POST	<code>/api/account/ops/orders/{order_no}/refund-abandon</code>	终止退款：失败态回已支付；处理中与未知态拒绝
POST	<code>/api/account/ops/orders/{order_no}/refund-offline-confirm</code>	线下打款确认：台账语义，幂等
GET	<code>/api/account/ops/orders/{order_no}/refund-risk</code>	审批前风险画像（只读）
GET	<code>/api/account/ops/orders/refunds/offline-pending</code>	待线下打款核对清单（与 5.2 同源）

- 运营面端点的统一索引与鉴权分组登记在运营管理域；运营发起退款不受门户频控约束。
- 出款类操作人身份比对口径：账号内用户取用户标识，外部操作人取带前缀的引用标识，二者皆无取匿名；「不同操作人」即标识不相等。

6. 关键约束与验收标准

6.1 约束

- 申请不动钱：申请与驳回只改订单状态，不写流水、不动余额；资金动作只发生在审批出款与人工结清；可退额度 = 订单金额 - 累计已退，两道都校验，无全局常量上界。
- 金额定格不可漂移：本次定额在审批时确定并落订单行，重试与人工结清一律沿用，复审只能审定格值。
- 四眼原则不可退化：需二审的单必须由两个不同操作人标识先后审批；首审批人不得自行复审；同人重试按幂等返回而非放行。
- 出款资格统一：出款类端点在两条令牌路径上共用同一份资格事实（在册 + 在用 + 持有出款权限），资格回收与停用即时生效。
- 不确定即不收敛：渠道报成功但实退金额无法核实时保持处理中并告警，绝不以本地定额自证冲销。
- 失败与未知账务等价：两类状态都不冲销，区别只在处置路径（失败可放弃、未知只能按账单核实结清）；重试一律沿用同一退款请求号。
- 幂等键是请求号不是订单终态：部分退款完成后订单回到已支付态，故幂等一律以退款请求号与冲销流水唯一索引承载。
- 对账同源同渠道：两侧必须同一渠道、同一自然日（本地按中国标准时间归日），本地侧不得按渠道全集过滤，同日重跑结果一致；本地流水找不到对应订单行时必须显式落为孤儿差异。
- 对账可重试与终态分清：账单未生成、网络类暂态失败可重试并有次数上限；凭据失效、渠道不支持、账单日非法为终态，告警后当日落定，不留无出口的空转。
- 线下确认不动账：清单与确认动作只承载执行台账，不改状态、不写流水、不动余额。
- 只回现金：不恢复赠金、不动信用额度；退款可把现金推为负，负债回潮交由欠费标记的单一重算规则处理。

6.2 验收标准

#	验收口径
1	非已支付状态或非充值类型订单申请退款：拒绝，状态不变、无流水落库、不进入待审批；剩余可退为零时同样被拒

#	验收口径
2	同一客户滚动 24h 内申请次数达上限：门户路径被拒、运营路径不受限；同单驳回后冷却窗内再次申请被拒
3	审批定额超过剩余可退或精度超过等效 2 位小数：拒绝且不落款、不改状态
4	首笔大额退款（达阈值）：返回待二审，订单保持待审批、不落流水、余额不变
5	第一审批人自行复审或换金额复审：均不给过且标记保留；第二位操作人按定格金额复审：出款成立、标记清空
6	部分退款出款成功：累计已退等于本次定额、订单回已支付、剩余可退为差额并可再审批；全部退完后置已退款终态、再申请被拒
7	渠道明确拒绝：置失败并带归一原因码、余额与流水均不变、产生告警
8	渠道报成功但实退金额不符：不冲销、转结果未知、出告警与审计；查询不可用或网络异常：保持处理中交轮询收敛，绝不置失败
9	未知单按「线下已打款」结清被拒、按「渠道账单核实已退」结清成功且幂等；处理中订单终止或人工结清均被拒；可能已退过的原因终止被拒而重试可行
10	轮询：自最近尝试起超 24 小时无结论的单转结果未知并告警且不再查询；同日重复触发不产生新流水与状态变更
11	并发两次收敛同一笔退款：恰有一条冲销流水、累计已退不重复累加，后到者返回幂等
12	对公转账审批通过即冲销并进入待线下打款清单（未确认视图），确认后转入已确认视图且不产生新的资金动作
13	对账：本地侧只统计本次对账渠道（另一渠道不落假差异）；渠道独有行为账单独有、本地流水无对应订单行时归为孤儿差异且不被忽略；两侧皆同时平账并同日重跑一致
14	渠道无账单能力时跳过且不计失败；暂态失败在累计重试达上限后当日落定并告警、终态失败告警后当日落定、跨日计数归零
15	全程落审计（申请 / 驳回 / 首审批 / 复审 / 退回 / 放弃）；出款类端点缺操作人、非标识格式、不在册、已停用或无出款权限时一律按无权限拒绝；凭据缺失的网关型退款直接置失败且不动账

6.3 待后续设计细化的开放项

1. 自动退款（无人工审批的小额自动放行）的阈值分级与风控信号闭环。
2. 退款通知的通道编排与去重窗口：站内信同事务落库、外部通道异步发送的失败重投口径。
3. 人工结清的复核留痕升级：现为单操作人动作，是否纳入双人复核。
4. 对账差异处置台账的处置状态回写与关闭条件（依赖风控与合规域的处置台能力）。