OYO AI

USE CASE

USE CASE · FINTECH FRAUD AND DISPUTES

From first report to regulator response

A single system of record for fraud, scam and dispute cases at a retail bank on OYO AI: one case from any channel, a containment playbook with a visible clock, a documented money trail, liability concluded against the bank's own controls, remediation under second-person approval, a customer restriction register, and regulator deadlines that escalate before they are missed.

INDUSTRY	SCOPE	PUBLISHED
Fintech · retail banking · fraud and disputes	12 use cases · 14 rules · 20 acceptance scenarios	5 November 2026

oyoai.com/use-cases/fintech-fraud-disputes

Contents

1 How to read this document

2 The gap it closes

3 Report and assess

4 Contain

5 Investigate

6 Decide

7 Restrictions (STOP)

8 Respond

9 Govern

10 Rules and clocks

11 Targets and how they are measured

12 Acceptance scenarios

13 Screens from the system

1 How to read this document

Each use case follows one piece of work through the system: who starts it, what happens, what the system refuses, and how acceptance proves it.

> **WHERE IT STANDS**
> The requirements are written and the solution is prepared for user acceptance testing on representative test data. The figures in section 11 are targets, not results.

In the flow diagrams: ● A person acts ● The system acts by itself ● A rule that can refuse

The roles

Role	What they do in the system
Intake officer	Registers reports, captures statements, requests immediate blocks.
Fraud analyst	Triage, money trail, control checklist, liability proposal, customer correspondence.

Role	What they do in the system
Head of Fraud and Disputes	Priority overrides, containment oversight, workload, escalations.
Channel operations officer	Applies and lifts restrictions, records identification evidence.
Remediation committee member	Approves or declines remediation decisions.
Compliance officer	Regulator and Mediator responses, AML referral.
Legal liaison	Police referrals, information requests, criminal case references.
Fraud business analyst	Maintains patterns, playbooks, restriction categories, control codes and deadline policy.
Internal auditor	Read and export everywhere, update rights nowhere.
System administrator	Users, roles and environment operations.

2 The gap it closes

Banks buy detection. What happens after a suspicion exists usually runs on tickets, mailboxes and memory, and that is where the operational and supervisory exposure sits.

A customer reports a scam by telephone, at a branch or in the app. The receiving officer records what they can in whatever tool is at hand. A block is requested by telephone and logged in a spreadsheet. The money trail is rebuilt by hand in a working file. Recall requests are tracked in the sender's mailbox, remediation lives in committee minutes, and regulator deadlines are remembered rather than tracked.

Today	On OYO AI
A report exists as a ticket, a call note and an e-mail thread	One case with one reference, visible to everyone who needs it
Containment depends on who answers the telephone	A playbook fires on assessment; the clock is visible and escalates itself
A restriction lift is a spreadsheet row	A lift cannot be completed without an identification method and an evidence reference
A repayment freeze lives in committee minutes	A register with per-customer terms, expiry dates and approvals
Regulator deadlines are tracked informally	Deadlines are computed from the bank's own policy and escalate before they are missed
Whether a control fired is reconstructed afterwards	The control checklist is completed in the case, while the facts are fresh
Policy changes wait for a software release	The fraud unit changes scoring, patterns and playbooks itself, the same day

Why now

Since 1 July 2026 Armenian financial institutions must offer the Central Bank's "STOP" mechanism: a customer can restrict remote services, and the restriction can only be lifted after the customer is identified. That is an evidence requirement, and evidence not captured at the moment of the action cannot be reconstructed later. Elsewhere the pressure is the same: UK Finance counted £576.4 million lost to authorised push payment scams in 2025, and instant payment rails keep shortening the window in which money can still be recovered.

What it deliberately does not do

- It does not detect fraud, score live transactions or take part in payment authorisation. It consumes signals from the platforms that do.
- It does not change core banking, the card switch or the lending platform. It holds decisions; the systems of record execute them.
- It does not post refunds, waivers or freezes to customer accounts. They are recorded as decisions and posted by the existing teams.
- It never stores full card data or authentication credentials.

3 Report and assess

UC-01

Register a fraud report

Primary actor	Intake officer
Trigger	A customer reports that money has left their account without their authorisation, or a referral arrives from the regulator, the Mediator or the police
Precondition	The customer is identified per branch procedure

Main flow

1. The officer opens intake and identifies the customer.
2. Captures the incident time, the disputed amount and the customer's own statement, in the customer's language.
3. Records whether a credit facility was drawn as part of the incident, with its reference and disbursement time.
4. Selects the apparent fraud pattern and attaches supporting material.
5. If funds may still be recoverable, requests an immediate restriction.
6. Submits. One case exists with a unique reference, in the analyst queue, with the clocks running.



Alternative flows

Existing open case	The officer is shown it and may attach the new information instead of creating a duplicate.
Different language	All customer-facing output follows the customer's language, not the operator's.
Regulator referral	The statutory response clock starts at the moment of receipt and is attached at intake.

RULES IT ENFORCES

- The stored statement is retained unaltered for the life of the case.
- Every action, decision and attachment goes on the case timeline.

WHAT PROVES IT A report from each channel produces one case with one reference and its source recorded. A second report inside the duplicate window prompts the officer.

UC-02

Assess and prioritise a case

Primary actor	Fraud analyst, system-assisted
Trigger	A case is created

Main flow

1. The system derives a priority from the pattern, the signals available, the recoverable amount and whether a facility was involved.
2. The target containment time is set from policy.
3. The case is routed: above the containment threshold to containment, otherwise to investigation.

Derive priority → Set target time → **Threshold** → Route

Alternative flows

Priority override	The Head of Fraud and Disputes changes it, recording a reason. An override without a reason is refused.
New information	The case is re-assessed and the change is visible on the timeline.

WHAT PROVES IT Two seeded cases differing in one factor receive the documented priorities.

4 Contain

UC-03

Contain an active incident

Primary actor	The system, with fraud analyst oversight
Trigger	A case is assessed above the containment threshold

Main flow

1. The playbook of the identified pattern is applied without further authorisation.
2. The defined service categories are restricted and the restriction is registered.
3. The disputed disbursement is flagged for hold.
4. A recall request is raised for every first-hop receiving institution holding traced funds.
5. Channel operations and the Head of Fraud and Disputes are notified.

Apply playbook → Restrict services → Flag hold → Raise recalls → Clock escalates

Alternative flows

Already restricted	If the customer restricted the services themselves, the existing restriction is referenced, not duplicated.
Institution unknown	The recall is deferred and raised from the investigation screen.
Recall unanswered	It is chased at the configured interval and escalated after the configured number of attempts, each attempt recorded.

WHAT PROVES IT A high-priority case shows its restrictions, recalls and target time within one refresh of assessment.

5 Investigate

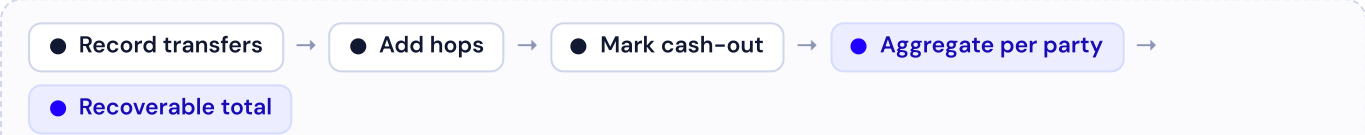
UC-04

Build the money trail

Primary actor	Fraud analyst
Trigger	Investigation begins

Main flow

1. The analyst records each transfer: institution, masked account, amount, time.
2. Adds later hops as information arrives from the customer or counterpart institutions.
3. Marks cash-out points.
4. Requests recalculation and reviews the aggregate at each party and the remaining recoverable total.



Alternative flows

Split transfers	The same party reached by two transfers: the aggregate is the sum of both, not the larger.
Funds loop back	The loop is flagged as an indicator and the calculation still completes.
Repeat party	A party appearing in more than one case within the configured period is highlighted.

WHAT PROVES IT For a seeded case with two transfers to one party, the aggregate equals their sum.

UC-05

Complete the control checklist and conclude liability

Primary actor	Fraud analyst
Trigger	Sufficient facts are known

Main flow

1. The system presents the controls expected for this pattern.
2. For each, the analyst records whether it acted and attaches the evidence reference.
3. The analyst concludes on liability and justifies the conclusion.
4. Submits the investigation. The case moves to decision.



Alternative flows

Refused submission	An incomplete checklist, a missing conclusion or a justification below the minimum is refused, with a message naming the deficiency.

RULES IT ENFORCES

- A conclusion of bank control gap is permitted only where the checklist shows a control that was expected to act and did not.

WHAT PROVES IT Selecting bank control gap where the checklist shows no gap is refused.

UC-06

Refer a case to the AML function

Primary actor	Fraud analyst or compliance officer
Trigger	The trail shows a mule pattern or another laundering indicator

Main flow

1. The analyst marks the case for AML referral with a reason.
2. The AML function receives the case with its parties, amounts and trail.
3. Both files retain the other's reference.



RULES IT ENFORCES

- Neither file can be edited to remove the other's reference.
- The customer's remediation entitlement is assessed independently of the laundering suspicion.

WHAT PROVES IT The referral appears in both files and is traceable in both directions.

6 Decide

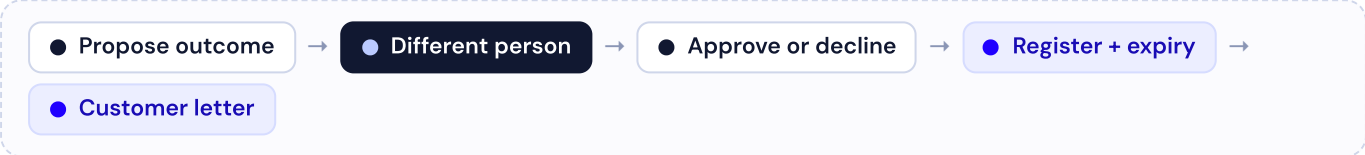
UC-07

Propose and approve remediation

Primary actor	Fraud analyst proposes, a remediation committee member approves
Trigger	The investigation is submitted and remediation is warranted

Main flow

1. The analyst proposes an outcome (repayment freeze, interest waiver, goodwill payment, full refund or decline) with terms and a rationale.
2. A different committee member reviews the case file and approves or declines with a note.
3. On approval the decision enters the register with its expiry date.
4. The customer letter is produced in the customer's language, including the reasoning and escalation rights.



Alternative flows

Self-approval	The proposer or the investigator attempts to approve: refused.
Declined	The decline letter is produced with the reasoning.
Freeze expiring	The responsible team is alerted at the configured lead time, and the expiring population is reportable.

WHAT PROVES IT An attempt by the investigator to approve is refused. Approval by another authorised person succeeds and the register shows terms, expiry, proposer and approver.

7 Restrictions (STOP)

The restriction lifecycle is deliberately independent of any fraud case, because a customer may raise or lift a restriction with no case in existence. It is the shortest process in the system and the one most likely to be inspected.

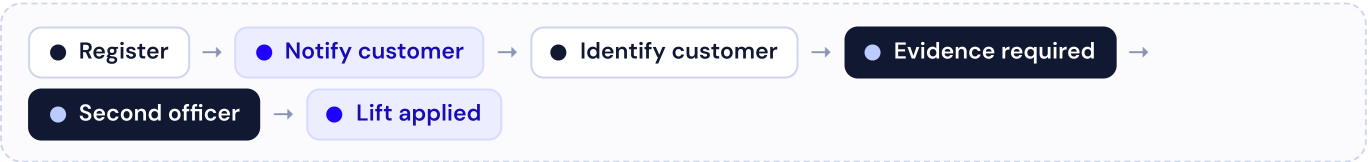
UC-08

Apply and lift a restriction

Primary actor	Channel operations officer
Trigger	A customer asks for a restriction to be applied or lifted
Precondition	For a lift, an active restriction exists

Main flow

1. The restriction is registered with its scope, origin, responsible officer and time, whatever channel it came through.
2. The customer is notified in their own language.
3. When a lift is requested, the officer identifies the customer by an approved method.
4. The officer records the method and the reference to the retained evidence, then submits.
5. Where the restriction is high-risk or case-linked, a different officer approves.
6. The lift is applied and the customer is notified.



Alternative flows

No evidence	The lift cannot be completed. The attempt itself is recorded.
Same officer	The same officer attempting both roles on a case-linked lift is refused.
New category	The list of restrictable services is business configuration, so a category the bank adds appears at once in the form and in reporting.

WHAT PROVES IT An export of a quarter's lifts shows method, evidence reference, approver and timestamps for each.

8 Respond

UC-09

Answer a regulator or Mediator request

Primary actor	Compliance officer
Trigger	A request is received from the regulator, the Financial System Mediator, the police or a court

Main flow

1. The request is registered with source, reference and receipt date.
2. The deadline is computed from policy and the working-day calendar.
3. The request is linked to the relevant cases.
4. The response is drafted, reviewed and approved.
5. The structured response document is produced and retained against the request and the case.

Register → Compute deadline → Link cases → Escalate → Approve response → Retain

Alternative flows

Deadline approaches	Escalation fires at the configured points, by default 50%, 80% and 100% of the window.
Deadline passes	The request is marked overdue and a breach is recorded with a reason code.

RULES IT ENFORCES

- Deadlines are policy values owned by the bank, never embedded in software.
- Three working days means working days, against the public-holiday calendar.

WHAT PROVES IT A deadline spanning a public holiday is computed correctly. Changing a policy value changes future deadlines only.

9 Govern

UC-10

Change a fraud pattern and re-assess parked cases

Primary actor	Fraud business analyst
Trigger	A new scam pattern appears, or a supervisory letter changes expectations

Main flow

1. The analyst opens the pattern catalogue.
2. Edits the weight, the containment playbook or the required controls, or adds a new pattern.
3. Saves. The change is versioned and audited, and material changes go to the Head of Fraud and Disputes for approval.
4. Requests re-assessment of open and parked cases and reviews what changed.



RULES IT ENFORCES

- Each case records which version of the configuration produced its outcome.

WHAT PROVES IT After a weight change, at least one parked case changes priority and enters containment, and the audit shows both values and the actor.

UC-11

Produce evidence for internal audit or a supervisor

Primary actor	Internal auditor
Trigger	An audit review or a supervisory request

Main flow

1. The auditor selects a period and a register.
2. Reviews the records on screen.
3. Exports the register and the associated audit trail.



WHAT PROVES IT An export exists showing, per record, who did what, when, and against which version of policy.

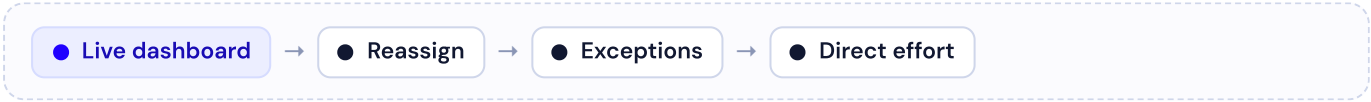
UC-12

Manage the workload of the unit

Primary actor	Head of Fraud and Disputes

Main flow

1. Reviews the dashboard: open cases by priority, clocks at risk, breaches, recovery in the period.
2. Reassigns cases, with the reason recorded.
3. Reviews the exception registers.
4. Directs effort at the patterns causing the largest losses.



WHAT PROVES IT Every dashboard element is populated from live data and responds to the filter.

10 Rules and clocks

The rules the system enforces

#	Rule	Why
1	A restriction may be lifted only after the customer is identified by an approved method and the evidence reference is recorded.	The direct requirement of the mechanism
2	The person who investigates a case may not approve its remediation.	Separation of duties on the individual case
3	No case is closed automatically. A decision to take no action is a recommendation by a named officer.	A machine may not dispose of a complaint
4	Every remediation decision carries a proposer, an approver, a written rationale and, where applicable, an expiry date.	Consistent, defensible treatment
5	Amounts reaching a party are aggregated across every path of the money trail.	Split transfers are the normal pattern
6	Bank control gap is permitted only where the checklist shows a control that should have acted and did not.	Prevents over- and under-attribution of fault
7	Deadlines are policy values owned by the bank and computed in working days where the obligation says so.	The bank owns its interpretation
8	The list of restrictable services is business-maintained. Extending it needs no release.	The regulation permits extension
9	An AML referral keeps its reference on both files.	Traceability across functions
10	Remediation entitlement is assessed independently of a laundering suspicion.	A third party's suspicion is no reason to withhold a remedy
11	Access is limited to the responsible branch, except oversight roles.	Least privilege with workable oversight
12	Nothing recorded here alters balances, postings or facility terms.	Preserves the systems of record
13	Case records, registers and their audit history are never deleted. Closure is a state.	Retention and reconstruction
14	Every configuration change is versioned, and each case records which version produced its outcome.	Answers why a case was scored differently in June

The clocks

All values are configuration, owned by the bank. No statutory value is embedded in software.

Clock	Starts at	Indicative default	Escalation	Owner
Containment, high priority	Case assessment	4 hours	50% and 100% of the window	Head of Fraud
Investigation	Case assignment	3 working days	On expiry	Head of Fraud
Recall response	Recall sent	24 hours	Chase, escalate after three attempts	Fraud analyst
Regulator or Mediator response	Receipt of the request	Set by Compliance	50%, 80%, 100%	Compliance officer
Customer evidence	Request issued	Bank policy	On expiry	Fraud analyst
Restriction lift decision	Lift requested	Bank policy	On expiry	Channel operations

11 Targets and how they are measured

> **THESE ARE TARGETS**
>
> The baseline is measured during discovery. Where the bank does not measure something today, the first release establishes the measurement.

Objective	Measure	At 6 months	At 12 months
Contain faster than funds move	Share of high-priority cases contained within the internal target time	70%	85% or more
Recover more of the loss	Recovered amount against gross reported loss	+15% relative	+30% relative
Evidence every lift	Share of lifts with identification method, evidence reference and required approval	100%	100%
Meet every deadline	Missed regulator, Mediator or police deadlines per quarter	1 or fewer, each explained	0, each exception explained
Administer remediation consistently	Share of decisions with proposer, approver, rationale and expiry	100%	100%
Reduce manual effort	Analyst hours per closed case	-20%	-40%
Change policy at regulatory speed	Time from a policy decision to it taking effect	Same day	Same day
Make performance visible	Management pack produced without manual compilation	Monthly	Monthly, plus on demand

The chain



12 Acceptance scenarios

Acceptance is demonstrated on synthetic data, with the bank present, by the bank's own staff wherever the criterion concerns a business action.

#	Scenario	Expected outcome
1	A report for a customer whose facility was drawn by a third party	One case with statement, facility details and customer language, in the analyst queue
2	Two reports for the same customer within the duplicate window	The second prompts the officer with the existing case
3	A high-priority case is assessed	Containment applied per the playbook, recalls raised, target time set
4	A trail with two parallel transfers to one party	The aggregate equals the sum; the recoverable total is shown
5	A trail containing a loop	The loop is flagged and the calculation completes
6	An investigation with an incomplete checklist	Refused, with a message naming the deficiency
7	Bank control gap where the checklist shows no gap	Refused
8	A lift with no identification evidence	Cannot be completed; the attempt is recorded
9	A case-linked lift approved by the officer who applied it	Refused; approval by a second officer succeeds
10	Remediation with the committed freeze term is approved	Register shows terms, expiry, proposer, approver; letter in the customer's language
11	The investigator approves their own proposal	Refused
12	A regulator request passes its deadline	Marked overdue, breach recorded with reason, owner alerted
13	A deadline spans a public holiday	Computed on working days per the calendar
14	A pattern weight and playbook change, then parked cases are re-assessed	At least one case changes priority and enters containment; audit shows both values
15	A business user adds a restriction category	Appears immediately in the form and in reporting
16	Internal audit exports a quarter of lifts	Method, evidence reference, approver and timestamps for each
17	A branch user tries to retrieve another branch's case	Refused through every route, including export
18	All dashboard elements are opened for the default period	Every element populated and responding to the filter
19	Each customer document is produced in all three languages	Content equivalent and correctly rendered

#	Scenario	Expected outcome
20	The monthly pack is generated and re-opened a week later	It reproduces identically

How it is delivered

Phase	Content	Duration
Discovery	Deadline values, identification methods, patterns, volumes, migration inventory	1 week
Pilot	One process end to end on test data. On the final day the bank's own analyst makes a live configuration change.	4 to 8 weeks
Phase 1	Intake, assessment, containment, restrictions, investigation, remediation register, customer letters, dashboard	About 6 weeks after pilot acceptance
Phase 2	Regulator and Mediator desk, exception registers, management pack, AML referral	About 4 weeks
Phase 3	Read-only interfaces to transaction and channel data; central restriction platform when published	Scoped separately

Deployment is inside the bank's perimeter. Integration is read-only in Phases 1 and 2, every interface falls back to manual entry, and no case can be blocked by an unavailable interface. Screens, messages, customer documents and reports exist in Armenian, Russian and English.

13 Screens from the system

Screens from the system, with sample data. Names are masked.



Command centre
Net loss, open cases and containment within target, with cases by branch, fraud pattern and severity. Every chart filters the whole board.



Loss and recovery by fraud pattern

Gross loss by pattern and containment outcome, case counts, and loss by liability conclusion.



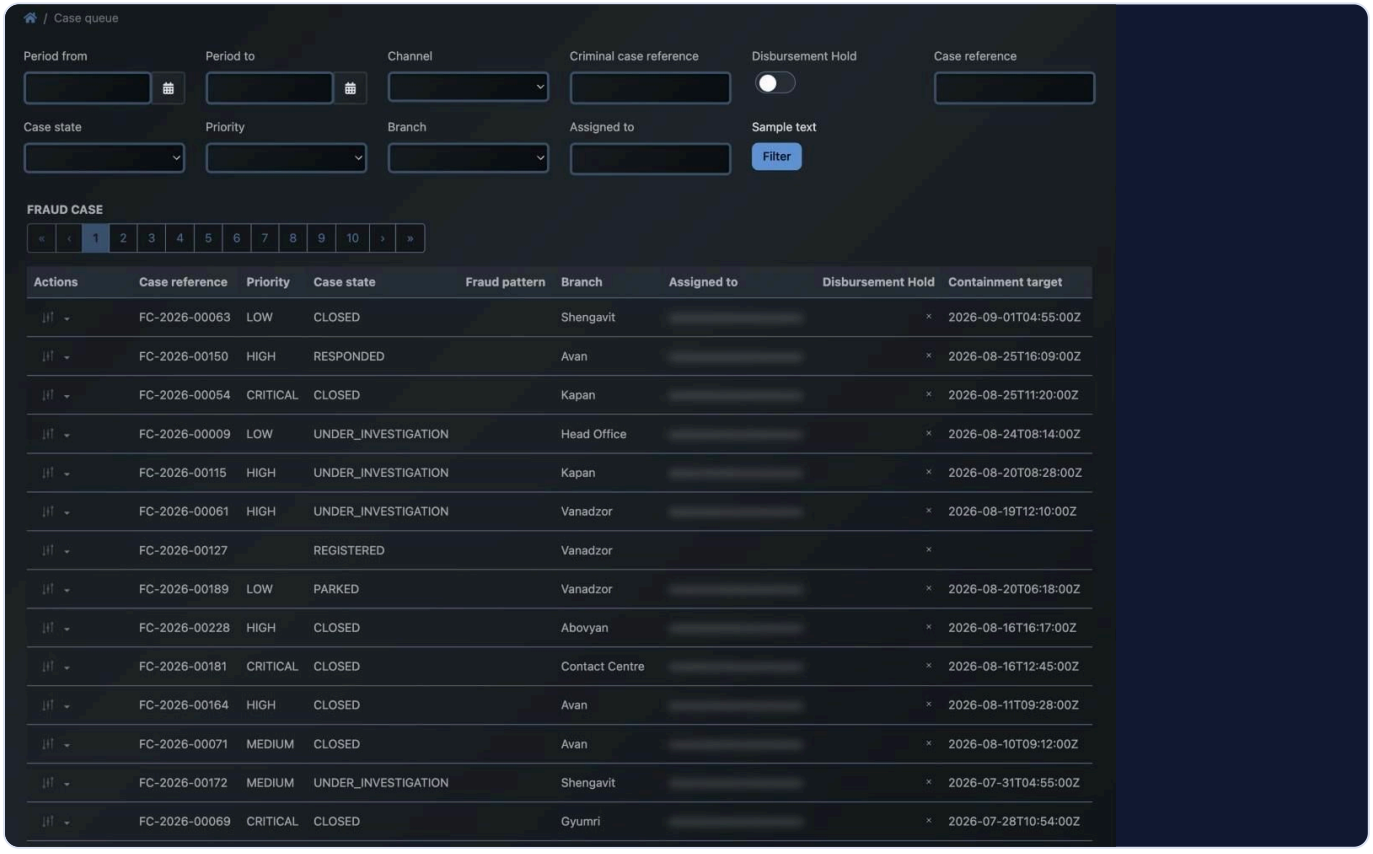
Regulatory clock compliance

Requests answered on time or overdue by source, the compliance verdict, and how late the overdue ones are.



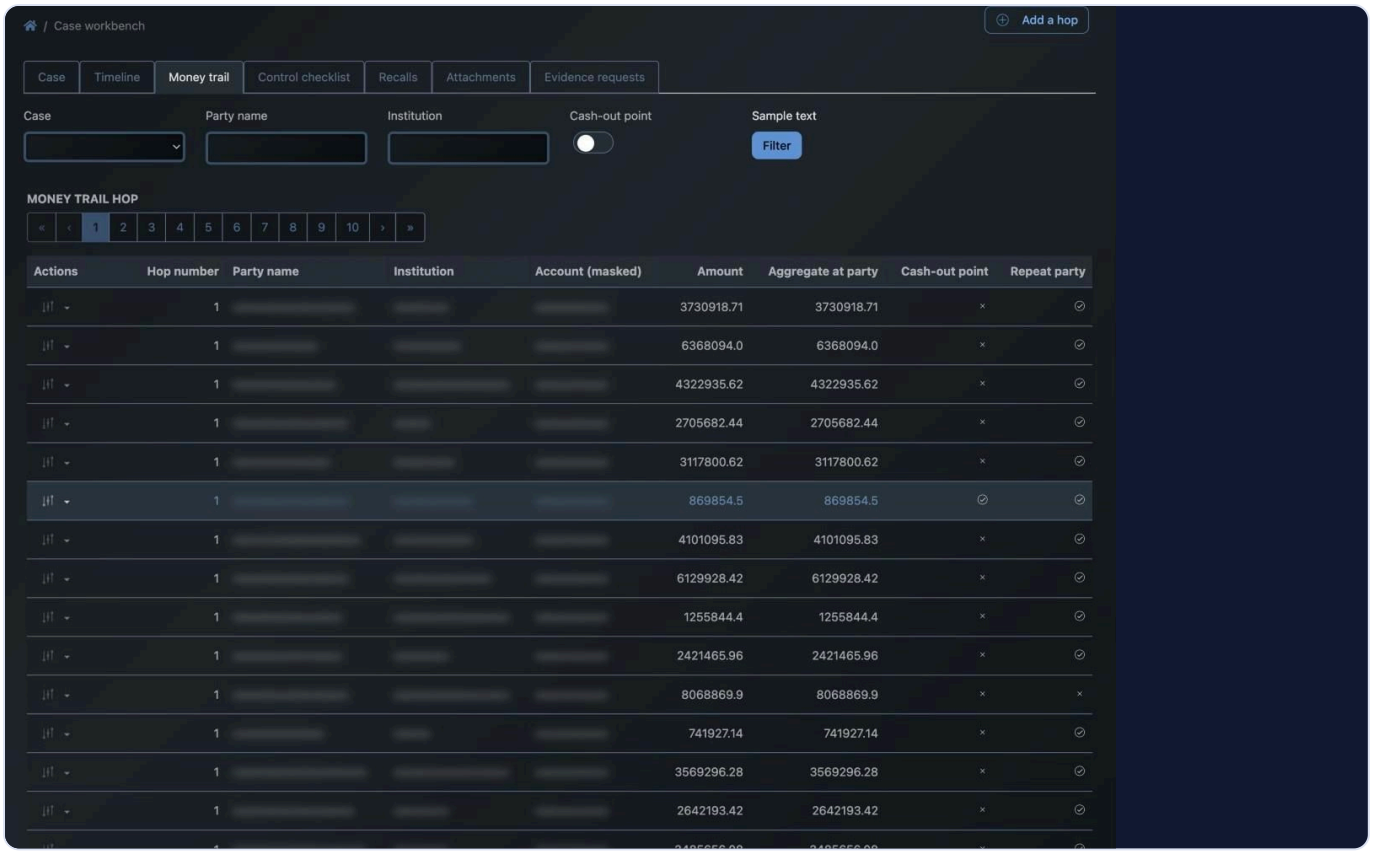
The money and the open clocks

Loss, cases and recovery rate by month, then open high-priority cases, breached clocks and containment by severity.

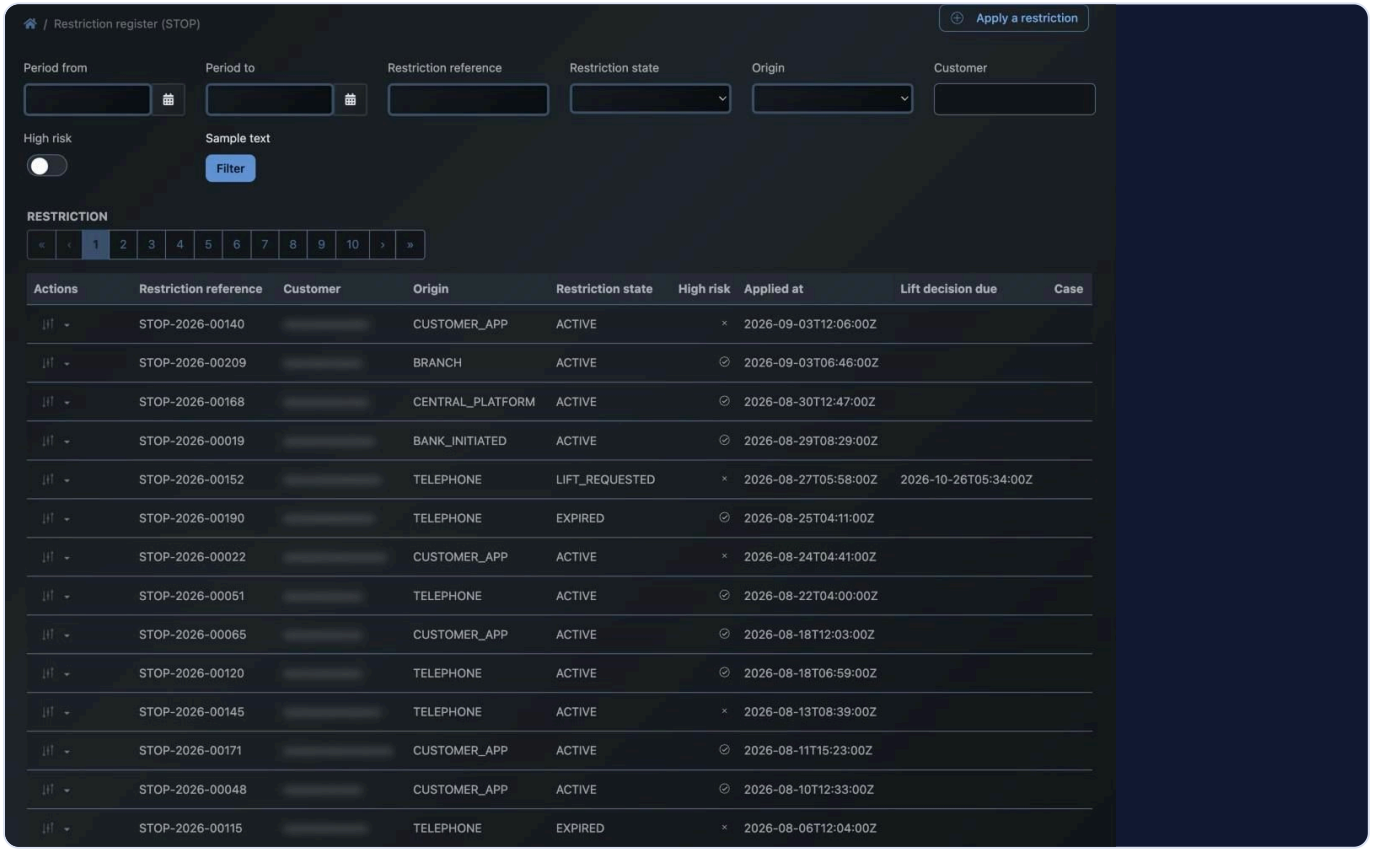


Case queue

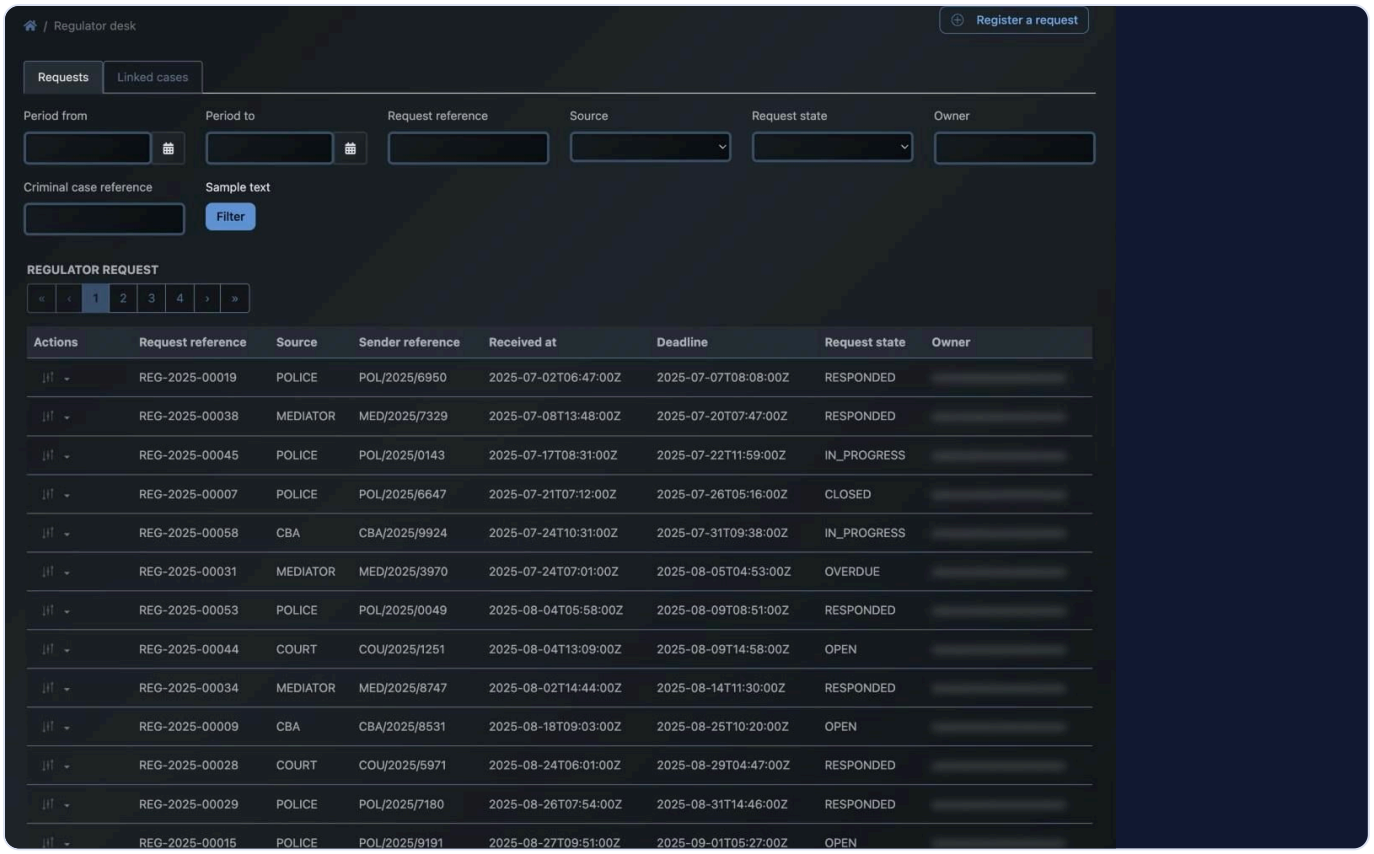
Every case with its priority, state, branch, assignee, disbursement hold and containment target.



Money trail
Each transfer hop by hop, with the aggregate at each party, cash-out points and repeat parties flagged.



Restriction register (STOP)
Every restriction with its origin, state, high-risk flag, applied time and lift decision deadline.



Regulator desk
Requests from the police, the Mediator, the Central Bank and the courts, each with its sender reference, deadline, state and owner.

About this document

Compiled in November 2026 from the requirements written with a retail bank for its fraud and disputes unit. The bank is not named and its own figures are left out. The solution is prepared for user acceptance testing on representative test data, with no connection to bank systems. Every outcome figure in this document is a target set in the requirements and measured against a baseline taken in discovery. None of them is a measured result yet. The screens at the end of this document show the system with sample data, with names masked.

OYO AI

Own your operations.

OYO AI is the AI business and process intelligence platform: no-code apps, business process automation and real-time process intelligence on one governed data model. The use cases in this document are built on it as configuration, not as customised code. What the system refuses, it refuses for every customer.

BOOK A WALKTHROUGH

oyoai.com/demo

WRITE TO US

info@oyoai.com · +1 855 236 7725

THIS USE CASE ONLINE

oyoai.com/use-cases/fintech-fraud-disputes

OYO AI INC.

14340 Torrey Chase Blvd, Suite 200, Houston, TX 77014

No-Code / Low-Code Platform
Build internal tools, workflows and portals visually, governed by IT.

Business Process Automation
Automate multi-step processes, approvals and exceptions end to end.

Business and Process Intelligence
Turn operational data into confident decisions and surface bottlenecks in real time.

ERP
A modular ERP keeping finance, operations, inventory and production in sync.

AI Virtual Consultant
Round-the-clock intelligence that watches the business and recommends the next best move.