CUSTIE PLATFORM

Fraud Operations KPIs & Standard Operating Procedures

Fraud Operations & Trust and Safety

Confidential | Internal Use Only

Document Owner	Fraud Operations & Trust and Safety
Classification	Confidential - Internal Use Only

1. Purpose & Scope

This document defines the Key Performance Indicators (KPIs) and Standard Operating Procedures (SOPs) for the Custie fraud operations function. KPIs establish the performance benchmarks used to evaluate onboarding quality, decision accuracy, and platform integrity. SOPs define the repeatable step-by-step processes used to execute fraud operations consistently across the participant lifecycle.

2. Fraud Operations KPIs

The following KPIs will be tracked on a weekly basis throughout the active onboarding period. Each KPI is defined, benchmarked, and reported against actual performance.

2.1 KPI Definitions & Benchmarks

KPI	Definition	Target	Actual
True Positive Rate (TPR)	Percentage of reviewed applications correctly approved as legitimate participants	≥95%	100%
False Positive Rate (FPR)	Percentage of legitimate applicants incorrectly flagged or rejected	≤5%	0%
Approval Rate	Total approved applications as a percentage of total applications reviewed	Monitored	100%
Decline Rate	Total rejected applications as a percentage of total applications reviewed	Monitored	0%

Time-to-Decision (TTD) — Baseline	Elapsed time from application submission to final decision at pilot launch	≤3 days	3 days
Time-to-Decision (TTD) — Optimized	Elapsed time after data minimization control is implemented	≤2 days	2 days
TTD Improvement	Reduction in time-to-decision achieved through process optimization	≥25%	33%
Fraud Incidents	Confirmed fraud events attributable to onboarded participants	0	0

2.2 KPI Performance by Phase

The following table tracks KPI performance by reporting period

Period	Applications	Approved	TTD (Days)	TPR	Incidents
Jul 2025	9	9	3	100%	0
Aug 2025	19	19	2	100%	0
Sep 2025	14	14	2	100%	0
Oct 2025	7	7	2	100%	0
Nov 2025	2	2	2	100%	0

2.3 KPI Reporting Process

KPIs are tracked and updated on a weekly basis by the Fraud Operations Manager. At the end of each reporting week the following data points should be recorded:

- Total applications submitted that week
- Total approved and rejected
- Time-to-decision for each application reviewed
- Any fraud incidents or platform integrity events

3. Standard Operating Procedures

The following SOPs define the repeatable step-by-step processes used by the fraud operations function. Each SOP corresponds to a core operational workflow and is written to be executable at the analyst level with final decisioning held by the Fraud Operations Manager.

SOP 001: Onboarding Application Review

Applies to: All new participant applications submitted through the Custie platform.

1. Log into the internal admin portal and navigate to the pending review queue.
2. Open the oldest pending application first.
3. Review all submitted profile information for completeness and internal consistency.
4. For service providers: open and review the uploaded government-issued ID document. Cross-reference name, photo, and document authenticity against submitted profile information.
5. For brick-and-mortar providers: review business verification documents in addition to ID.
6. Assess stated purpose, services offered, and background information for legitimacy and platform fit.
7. Apply detection logic criteria from the Detection Logic Framework to identify any risk signals.
8. Render a decision: APPROVED or REJECTED.
9. Update the application status in the admin portal.
10. If rejected: document the reason and initiate participant notification through the platform.
11. Record TTD and outcome in the weekly KPI tracker.

SOP 002: Post-Onboarding Complaint & Abuse Review

Applies to: All participant complaints and platform abuse reports received after onboarding is complete.

12. Receive complaint or abuse report through the platform's internal reporting path.
13. Log the report immediately: participant ID, date received, nature of complaint, reporting party.
14. Triage the report against the detection logic risk signal table to assign risk level (High, Medium, Low).
15. If High risk: escalate immediately to Fraud Operations Manager before proceeding.
16. Whether Medium or Low: proceed with full review through the admin portal.
17. Review the reported participant's account record, onboarding history, and any prior complaints.
18. Review relevant messaging, activity, or behavior related to the complaint.
19. Document findings with sufficient detail to support decisioning.
20. Escalate to Fraud Operations Manager with findings summary and recommended action.
21. Implement the decision rendered by the Fraud Operations Manager.
22. Notify affected parties of the outcome through the platform.
23. Close the case and update the case record.

SOP 003: Weekly KPI Reporting

Applies to: Fraud Operations Team. Frequency: Weekly, every Monday covering the prior week.

24. Open the internal fraud operations KPI tracker in the risk metrics tracker.
25. Enter the week's application volume, approvals, rejections, and pending count.
26. Calculate and record approval rate, decline rate, TPR, FPR, and average TTD for the week.
27. Record any fraud incidents or platform integrity events (enter 0 if none).
28. Add relevant notes for any significant events, process changes, or anomalies.
29. Review trend data against prior weeks to identify any performance shifts.
30. If any KPI falls outside target threshold, document the variance and corrective action taken.

31. Prepare a summary of the week's performance for leadership communication if required.

SOP 004: Escalation to Leadership

Applies to: Any situation requiring leadership awareness or decision. Triggers defined in the Escalation Framework.

32. Identify that an escalation trigger has been met per the Escalation Framework.
33. Prepare an escalation summary in Slack including participant ID, nature of the issue, risk level, findings, and recommended action.
34. Tag the appropriate leadership contact and mark as urgent if High risk.
35. Await acknowledgment and direction from leadership.
36. Implement the directed action and document the outcome.
37. Update the case record and KPI tracker accordingly.