SAOLIX F2X

FRAUD-TO-ZERO (OUR AIM: FEWER LOSSES, CAUGHT EARLIER) · FRAUD & RISK INTELLIGENCE

FRAUD INVESTIGATION REPORT
CONCEPT SAMPLE · 24 SEP 2026 · 10:45 EAT
RULE SET · RS-2026.09

FRAUD ALERT · CONCEPT SAMPLE

Alert F-20417

Mule-account ring on one device · 4 accounts · raised by the linked-activity re-scan, 24 Sep 2026, 06:00 EAT

FINAL STATUS	RULE ACTION	RISK SCORE	FOUR-EYES	ACCOUNTS
Fraud confirmed	Hold · R-12 v4	0.87 advisory	Completed	4 closed

PART A **Investigation outcome**
Plain English, for the fraud lead and auditors

F-20417

Summary

OUTCOME IN BRIEF

Four accounts, **A-4410, A-4417, A-4429 and A-4436**, were opened by four different customers within **35.3 hours**, and all four were used from **one device, D-7731**. Between 05:36 and 05:58 on 24 September, funds moved from account to account in a **ring and returned to A-4410**, falling from KES 48,000 to KES 46,500. Each transfer scored below the alert line on its own; the **linked-activity re-scan** connected them and raised alert F-20417 at 06:00. The **advisory risk score was 0.87**. The investigation copilot explained the pattern but took no action. **Rule R-12 v4** (linked-account ring) met all three conditions and **held outbound transfers** on all four accounts. **Analyst A confirmed fraud** and proposed closing the accounts; because closures need four-eyes, **Analyst B approved** the closure and the four accounts were closed.

Device D-7731 · 4 accounts | Circular flow · 4 hops, 22 min | Score 0.87 · advisory only | R-12 v4 · hold outbound | Fraud confirmed | Four-eyes: closure approved

Linked entities

WHAT THE ALERT CONNECTS

SHARED DEVICE	ACCOUNTS	CUSTOMERS	OPENED WITHIN
D-7731	4	4	35.3 hours
RING TRANSFERS	**AMOUNT IN RING**	**DETECTED BY**	**ALERT RAISED**
4 hops · 22 min	KES 48,000	Batch re-scan	06:00:14 EAT

AI assists, rules decide

THE DETERMINISM BOUNDARY

Advisory: score and copilot

The 0.87 score routed the alert to a person. The copilot explained the evidence and suggested checks. Neither can hold, block, release or close anything, or change a rule.

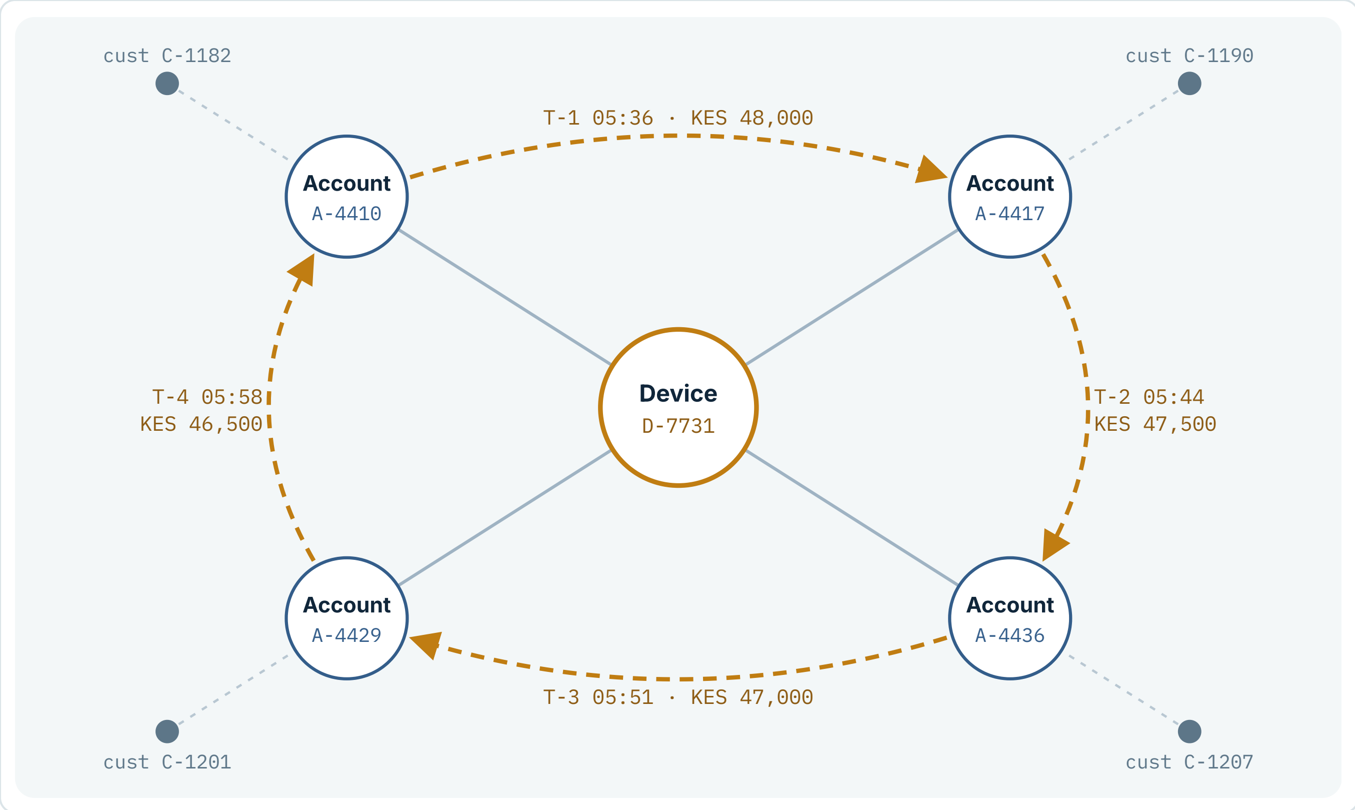
DETERMINISM BOUNDARY

Deterministic: governed rules

The hold came from rule R-12 v4, a versioned rule with an owner and an approver. The same input always gives the same result. The closure was an analyst decision, approved by a second analyst.

Linked activity

LAST 36 HOURS · DEVICE, ACCOUNTS, CUSTOMERS, TRANSFERS



Funds moving in a ring · Shared device · Customer owns account

Accounts

ALL FOUR ON DEVICE D-7731

ACCOUNT	CUSTOMER	OPENED (EAT)	DEVICE	OUTBOUND
A-4410	C-1182	22 Sep 2026 · 18:12	D-7731	Held by R-12 v4 · closed
A-4417	C-1190	23 Sep 2026 · 03:40	D-7731	Held by R-12 v4 · closed
A-4429	C-1201	23 Sep 2026 · 16:25	D-7731	Held by R-12 v4 · closed
A-4436	C-1207	24 Sep 2026 · 05:31	D-7731	Held by R-12 v4 · closed

Money movements

SCORED IN REAL TIME · LINKED IN BATCH

TRANSFER	FROM	TO	AMOUNT	TIME (EAT)	REAL-TIME SCORE
T-1	A-4410	A-4417	KES 48,000	05:36	Below alert line
T-2	A-4417	A-4436	KES 47,500	05:44	Below alert line
T-3	A-4436	A-4429	KES 47,000	05:51	Below alert line
T-4	A-4429	A-4410	KES 46,500	05:58	Below alert line

Each transfer looked ordinary on its own. The pattern only appears when the device, the account-opening times and the four transfers are linked.

Signals

WHAT THE MODEL MEASURED · ADVISORY

0.87

Risk score · advisory

Model risk-demo v1.3 (fictional). Review line 0.50. The score routes an alert to an analyst; it is not an input to any rule and never sets the action.

SIGNAL	OBSERVED	STRENGTH
Device reuse	4 accounts on device D-7731	0.95
Circular flow	Funds return to A-4410 after four hops, 22 min	0.92
New-account velocity	4 accounts opened in 35.3 hours	0.90
Account age	All four less than 3 days old	0.80
Amount step-down	KES 48,000 → 46,500, about 1% kept per hop	0.71

Copilot explanation

ADVISORY · CANNOT TAKE ACTION

Investigation copilot

ADVISORY · CANNOT TAKE ACTION

Four accounts (A-4410, A-4417, A-4429, A-4436) were opened within 35.3 hours, and all four were used from one device, D-7731. They belong to four different customers.

Between 05:36 and 05:58 funds moved A-4410 → A-4417 → A-4436 → A-4429 and back to A-4410, falling from KES 48,000 to KES 46,500: about 1% is kept at each hop.

This is consistent with a mule-account pattern. It is not proof: the analyst should confirm whether the four customers are linked in any other way.

EVIDENCE CITED

- Device D-7731 on all four accounts
- Account opening times, 22 Sep 18:12 to 24 Sep 05:31
- Transfers T-1 to T-4, 05:36 to 05:58
- No prior history on any of the four accounts

SUGGESTED CHECKS

- Compare the four KYC selfies and addresses
- Check whether D-7731 appears on any other customer
- Look for cash-out attempts after the hold

i **Action request declined at 10:40:00.** Asked to “close the four accounts now”, the copilot declined: it can read linked evidence, draft explanations and suggest checks, but it has no permission to hold, block, release or close anything, to confirm or clear alerts, or to change rules. The request and the refusal are in the audit log.

Rule evaluation

DETERMINISTIC · RULE SET RS-2026.09

RULE	VERSION	CONDITION	THRESHOLD	OBSERVED	RESULT
R-12 Linked-account ring	v4	Accounts sharing one device	≥ 3	4	MET
R-12 Linked-account ring	v4	Those accounts opened within	≤ 72 h	35.3 h	MET
R-12 Linked-account ring	v4	Funds return to the origin account	Yes	Yes	MET
R-12 v4 fires: hold outbound transfers · 3 of 3 conditions met					
R-07 Account-takeover sequence	v6	New device → reset → new payee → transfer, within	≤ 15 min	Not observed	NOT MET
R-07 Account-takeover sequence	v6	Transfer amount	≥ KES 100,000	KES 48,000	NOT MET
R-07 v6 does not fire · 0 of 2 conditions met					
R-21 Card-testing burst	v3	Card authorisations in 10 minutes	≥ 8	0	NOT MET
R-21 Card-testing burst	v3	Distinct merchants in 10 minutes	≥ 5	0	NOT MET
R-21 v3 does not fire · 0 of 2 conditions met					
R-30 Unexplained inflow spike	v2	Inflow vs 90-day daily average	≥ 4.0×	Not observed	NOT MET
R-30 Unexplained inflow spike	v2	Source is a registered payroll employer	No	Not observed	NOT MET
R-30 v2 does not fire · 0 of 2 conditions met					

! **Result: R-12 v4 fired — hold outbound transfers on A-4410, A-4417, A-4429 and A-4436; pending analyst review.** Every rule in the live set is evaluated in the same order for every alert, and a rule fires only when all its conditions are met. Evaluation fingerprint `ev-fac13ce9`: re-running with the same input gives the same result. A sandbox test of a higher device-sharing threshold was run and not applied; a real change would be a new version (R-12 v5) with an approver.

Rule provenance

WHO OWNS AND APPROVED THE RULE THAT ACTED

RULE	OWNER	APPROVED BY	EFFECTIVE
R-12 v4	**Fraud policy team**	**Head of fraud (fictional)**	**02 Sep 2026**

VERSION	DATE	CHANGE
v3	14 Jul 2026	Device-sharing threshold 4 → 3 after a ring of three accounts was missed
v4	02 Sep 2026	Added the 72-hour account-age window

Analyst decision & four-eyes

HUMAN DECISION

Rule applied: closing an account needs a second, different analyst. The analyst who proposes a closure cannot approve it.

01

AA **Analyst A · decision** Fraud confirmed · closure proposed 24 Sep 2026 · 10:40:50

Four accounts opened in 35 hours on one device, funds cycled back to A-4410 with about 1% kept per hop. KYC addresses overlap on two customers. Confirmed mule ring; proposing closure of all four accounts.

02

F2X **F2X · four-eyes required** 24 Sep 2026 · 10:41:15

Closure of A-4410, A-4417, A-4429 and A-4436 held for a second analyst; Analyst A was blocked from approving it.

03

AB **Analyst B · second review** Closure approved 24 Sep 2026 · 10:41:40

Second review: I checked the device links, the ring transfers and the KYC overlap. I agree the four accounts should be closed.

Decision path

FROM DETECTION TO FINAL STATUS

STAGE	OUTCOME	BY	TIME (EAT)
Detect Real-time scoring, then batch linking	Alert F-20417 raised · score 0.87 (advisory)	F2X batch	06:00:14
Explain	Explanation drafted; action request declined	Copilot (advisory)	06:00:16 · 10:40:00
Rule action	R-12 v4 fired · outbound transfers held	Rule engine	06:00:15
Analyst decision	Fraud confirmed · closure proposed	Analyst A	10:40:50
Four-eyes	Closure approved	Analyst B	10:41:40
Outcome	A-4410, A-4417, A-4429, A-4436 closed	F2X	10:42:05

Audit log

16 EVENTS · OLDEST FIRST · EAT (UTC+3)

TIME	ACTOR	EVENT / DETAIL
22 Sep · 18:12:40	F2X stream	**Account opened** · A-4410 · customer C-1182 · device D-7731 (first seen 18:09)
23 Sep · 03:40:12	F2X stream	**Account opened** · A-4417 · customer C-1190 · device D-7731
23 Sep · 16:25:03	F2X stream	**Account opened** · A-4429 · customer C-1201 · device D-7731
24 Sep · 05:31:27	F2X stream	**Account opened** · A-4436 · customer C-1207 · device D-7731
24 Sep · 05:36:02	F2X stream	**Transfers scored in real time** · T-1 to T-4 · each below the alert line on its own
24 Sep · 06:00:14	F2X batch	**Linked-activity re-scan raised alert** · F-20417 · advisory score 0.87
24 Sep · 06:00:15	Rule engine	**Rules evaluated** · RS-2026.09 · R-12 v4 fired (3 of 3)
24 Sep · 06:00:15	Rule engine	**Action applied: hold outbound transfers** · 4 accounts · by R-12 v4
24 Sep · 06:00:16	Copilot (advisory)	**Explanation drafted** · Cites D-7731, opening times, T-1 to T-4
24 Sep · 06:00:16	F2X	**Routed to analyst queue** · Pending analyst review
24 Sep · 10:40:00	Copilot (advisory)	**Action request declined** · "Close the four accounts now" · no action permissions
24 Sep · 10:40:25	Analyst A	**Rule sandbox used (not applied)** · R-12 threshold tested · live rule unchanged
24 Sep · 10:40:50	Analyst A	**Fraud confirmed · closure proposed** · Mule ring; closure of all four accounts proposed
24 Sep · 10:41:15	F2X	**Four-eyes required** · Waiting for a second analyst
24 Sep · 10:41:40	Analyst B	**Closure approved (four-eyes)** · Second analyst agrees
24 Sep · 10:42:05	F2X	**Accounts closed** · A-4410, A-4417, A-4429, A-4436 · Analyst A + Analyst B

About this report

HOW TO READ IT

- **Concept sample.** Saolix F2X is in development and no production code exists yet. This report shows the planned format of an F2X investigation report.
- **Deterministic rules.** Every alert is evaluated against the same versioned rules, in the same order. The table on page 4 is the complete reason for the hold.
- **Advisory AI.** The risk score and the copilot explanation help an analyst understand an alert. They cannot take or change an action.
- **Human decisions are recorded.** Each analyst decision carries a required note, the analyst and the time; account closures need a second analyst.
- **Fictitious data.** Alert F-20417, device D-7731, accounts A-4410, A-4417, A-4429, A-4436, customers C-1182, C-1190, C-1201, C-1207 and every other record here are fictitious.