

Fraud Pattern Miner

Find the fraud patterns in the event data you already have. Every finding comes with the reason and the records that prove it.

Fraud Pattern Miner reads the exports your systems already produce, rebuilds the behaviour behind them, and shows your fraud team which numbers, accounts and counterparties are worth a look, and why. It looks back at activity that has already happened. It runs where your data lives, and it never sends your records to an AI service.

It reads IVR call activity and account-to-account payments today, on the same engine and with the same promise.

Data shapes

Data shape	What it reads	Availability
IVR call activity	Call-event exports from your IVR platform	Available now
Account-to-account payments	ISO 20022 payment messages for one named scheme	Available now
Card authorisations	Card network messages	Next

The problem

A risk score tells you where to look. It does not tell you why. Fraud hides across thousands of records: one call or one transfer looks ordinary, but a hundred calls from one number cycling through card numbers do not, and neither does one account that receives money from nineteen others in an afternoon. Teams end up rebuilding incidents by hand, or they cannot move production data into a hosted tool at all.

What a finding looks like

Each finding answers five questions: what was flagged, when, which behaviour triggered it, how far it crossed the line, and which records prove it. The layout is the same in every shape.

IVR call activity

Calling number	tok:v2:8c41...e2 score 7.0, above the review line of 3.0
Window	3 Aug, 02:00 to 03:00
Pattern	Reconnaissance and enumeration
Why	One calling number tested several card or account targets. calls in the hour at least 3 observed 10 distinct card entries at least 3 observed 10
Evidence	10 supporting call IDs and the representative call path

Account-to-account payments

Receiving account	tok:v2:41f0...9a score 6.2, above the review line of 3.0
Window	3 Aug, 09:00 to 12:00
Pattern	Many accounts paying one account
Why	More paying accounts than this account's usual segment sees. distinct paying accounts at least 8 observed 19
Evidence	19 supporting transfers and the money-movement graph

Illustrative examples. Not real data.

What it looks for

IVR call activity

Pattern family	What it looks like in the logs
Caller identity and account takeover	An account reached from an unusually broad set of numbers, bursts of many numbers behaving alike, dense groups of linked numbers and accounts
Credential and servicing manipulation	Repeated failed validation, activation alongside other identity signals, a valid account entry followed by repeated transfers to an agent
Reconnaissance and enumeration	One number testing many cards or accounts, checking balances across targets or moving across dialled lines, a few numbers spread across many accounts
Automated calling and TDoS	Machine-regular keypad timing, call volumes above what normal traffic predicts, bursts on one line, calls with little or no interaction

Pattern family	What it looks like in the logs
Behaviour no rule describes yet	Call paths that are rare in normal traffic, outlier windows, and candidate rules discovered from your own data, kept out of scoring until a person reviews them

Account-to-account payments

Pattern family	What it looks like in the records
Mule account networks	Many accounts paying one account, or one account paying many, with observed transfers linking them
Rapid pass-through	Money that arrives in an account and leaves again within minutes
Authorised push payment and business email compromise	A large first payment to a new beneficiary, set against the amounts that account normally sends
Repeated just-under-threshold transfers	A run of transfers sized inside a band below a named scheme or policy limit
Unusual returns	Return rates or reason codes that depart from the reference
Behaviour no rule describes yet	Candidate rules discovered from your own data, selected independently of the authored rules and kept out of scoring until a person reviews them

For payments, legitimate accounts such as payroll, sweep, escrow and collection accounts behave much like mule accounts. The design takes a list of those account classes as an input so they are not flagged as lookalikes.

Your data stays yours

- **Local by design.** The analysis needs no internet connection and sends nothing out.
- **Only known fields pass.** Field content the miner does not recognise is dropped before analysis.
- **Identifiers become tokens.** Phone numbers, accounts and card fragments are replaced with keyed tokens (HMAC-SHA256). The key stays in your keychain or secrets store and never appears in a report.
- **Payments follow the same boundary.** Account and party identifiers become keyed tokens. Names, addresses and free-text remittance are discarded at the boundary. Card numbers and card security data are out of scope for the first payments release.
- **No AI model in the analysis.** Findings come from explicit rules and statistical methods, each shown with its threshold and the value observed, not from a language model.
- **Reproducible.** Every run is sealed with digests and records its configuration, so a finding can be checked and rerun later.
- **Built for regulated markets.** It supports the data minimisation and pseudonymisation that laws such as Nigeria's Data Protection Act 2023 expect, and follows NITDA's advice to keep personal data out

of public AI tools. It does not make you compliant on its own. It gives your data protection team fewer data flows to assess.

Two ways to use it

Both options cover each data shape as it becomes available.

Managed analysis: we run it, you get the reports

You reduce your export on your side with the reduction tool we provide. It applies the same privacy boundary as the analysis and tokenises identifiers with **your** key. You send us only the reduced files, through a transfer you approve. If no data can leave your premises, we work on a machine you control instead.

Your tokens pass through our analysis unchanged. Only someone holding your key and your original records can link a finding back to a customer or an account. We hold neither. The same reduction step applies to payment files.

You receive: an evidence bundle (readable HTML summary, full JSON report, and spreadsheets of findings, candidate rules and evidence), a walkthrough with your analysts, and a shortlist of candidate controls worth testing.

Best for: a first look, the weeks after an incident, a control review, or teams without in-house capacity.

Licensed platform: you run it

Your team installs the software on its own machines or internal network and runs every analysis itself.

You receive: the desktop app for analysts, a command line for scripted and scheduled runs, WebAssembly modules for embedding, user guides, signed releases, and updates and support for the licence term. Payments analysis comes in the same desktop app and command line.

Runs on: signed releases for macOS 12 or later today. Ask us about other platforms.

Best for: teams that cannot share data even in reduced form, recurring analysis, and in-house fraud engineering teams.

At a glance

	Managed analysis	Licensed platform
Who runs the analysis	We do	Your team
Where raw records stay	With you	With you
What leaves your network	Reduced, tokenised files, or nothing if we work on-site	Nothing

	Managed analysis	Licensed platform
Who holds the tokenisation key	You	You
What you receive	Reports, a readout and candidate controls	The software, guides, updates and support

How a first engagement runs

1. **Schema check.** A preflight reads your export's column layout, not its customer values, and confirms the miner can read it.
2. **Baseline.** If you have a period your team considers normal activity, we use it as the reference. If not, the miner cleans its own baseline in two passes. That is weaker than a reviewed period, and the report says so.
3. **Analysis and review.** Findings and candidate rules go to your analysts with the evidence attached.
4. **Measure.** We do not quote detection accuracy until it has been measured against your own confirmed cases. A pilot can measure it using your fraud team's case outcomes.

What we need from you

IVR call activity: call-event exports in the supported layout, as CSV or TSV files, folders or zip archives. Multi-gigabyte deliveries are fine, including a log split into chunks where only the first file carries the header. We also need the time zone your platform logs in, and a normal-activity reference period if you have one.

Account-to-account payments: the first release covers one named payment scheme and its declared ISO 20022 message versions. Tell us which scheme you operate on. Useful companions are a list of your payroll, sweep and collection account classes, and any confirmation-of-payee results you keep.

What it is not

It is not a real-time call or payment blocker, a caller-authentication product, or an autonomous fraud decision. A finding explains why the software flagged a window or a transfer for review. It does not prove intent or confirm that fraud occurred. Your analysts make that call.

For payments specifically, a score is a review priority, not a probability. It is not a regulatory report, and it does not replace your fraud, sanctions or anti-money-laundering controls.

Talk to us

If you want card authorisations sooner, or want to shape which payment scheme comes next, say so.

Write to hello@finesample.com.