FULL CASE INVESTIGATION

Priimal SignalCore

AI-scored, investigator-ready case management for telecom revenue leakage, sized for smaller MVNOs and carriers.

MVNOS | CARRIERS & INTERCONNECT

THE CHALLENGE

Smaller mobile virtual network operators and carriers often see the same revenue leakage as larger telcos, SIM box bypass, grey routing, traffic pumping, roaming abuse, but without the dedicated fraud management team or the CDR analytics stack that a Tier 1 carrier would run in house. The data exists in your call detail records and interconnect logs. What is missing is a practical way to turn it into a case a small team can actually work.

Signal Core is the part of Vantage that does that for you. You send your traffic and billing data in, the platform scores it, and your team gets a working case queue rather than a raw CDR export.

KEY CAPABILITIES

1 AI Risk Scoring, Built for Telco Revenue Leakage

Every record you upload or send through the API passes through Vantage's scoring pipeline. Records that show a pattern worth investigating are assessed by AI and, once they cross your configured threshold, set to 60 by default and adjustable per tenant, created as a case in your queue. Each case comes back with a risk score from 0 to 100, a risk band of critical, high, medium or low, a confidence level, one or more flags, and a plain English explanation of why it was flagged. An investigator can trigger a re-score on any case at any point and see the score history right on the case page. Scores are decision support for your investigators, not an automated decision: a case is reviewed by your team before any action is taken on it.

SIM Box | Bypass Fraud | Grey Route | Traffic Pumping | Roaming Fraud

2 Full Case Investigation Workflow

A sortable, filterable case queue sits at the centre of Signal Core. Every case can be assigned, re-assigned, moved through statuses such as open, under review and resolved, and set to a priority level. Investigators keep a threaded notes panel on each case, and any note can be marked internal only or left visible in the field work orders, with the author's name and timestamp attached automatically. Every meaningful action on a case, from a status change to a re-score, is logged to a full audit trail that sits alongside the case and travels with it into any export.

3 Assignment Alerts and a Personal Case Inbox

When a case is assigned to someone, an email goes out automatically, carrying your organisation's name alongside Vantage module branding, with the case reference, risk score, value at risk and a direct link, so nobody has to

check the platform to know work has landed on their desk. Each investigator also gets a personal "My Cases" inbox showing only their open and under review cases, sorted by priority and then by risk score, so the highest value work is always at the top. That matters for a lean MVNO team where one or two people cover fraud management alongside other duties.

4 Branded PDF Case Export

Any case can be exported as a PDF in one click, carrying your organisation's name alongside Vantage module branding. The export carries the risk score, identity and confidence details, the value at risk, a full AI explainability breakdown, the evidence table where one exists, the recovery log, every investigator note, and the complete audit trail. It gives a small fraud or revenue assurance team the same standard of documentation a larger carrier's in-house unit would produce.

5 Recovery Tracking

Once a recovery is confirmed, it gets logged against the case with the gross value recovered, giving you a clear, auditable record of what has actually been recovered rather than an estimate reconstructed after the fact.

6 Field and Network Dispatch

An administrator can manually trigger a dispatch directly from any case, sent as a signed, one-time request to whichever network operations, fraud management or ticketing system your team already uses, connected through a webhook you configure in settings. The dispatch, its destination and the response status are all recorded in the case's activity log, so there is never any doubt about whether it actually went out.

7 Natural Language Query

Instead of building a report or waiting on an analyst, anyone on your team can ask Signal Core a plain English question about their case data and get an answer straight back. For a small MVNO team without a dedicated data analyst, this is often the difference between checking a pattern the same day and not checking it at all.

8 REST API Access

Signal Core includes REST API access as standard, using a bearer token unique to your tenant. You can score a single record, or send up to 100 in one batch call, directly from your own billing mediation or CDR processing system. A public sandbox with pre-scored demo records and live documentation is available so your technical team can evaluate the API before committing to anything.

WHAT YOU RECEIVE

- **Case queue:** an AI-scored, prioritised list of traffic and account records worth investigating.
- **Explainability:** a plain English reason and flag breakdown behind every score, not just a number.
- **Full workflow:** assignment, threaded notes, status tracking and a complete audit trail on every case.
- **Branded exports:** case reports ready to hand to interconnect partners, regulators or auditors.
- **Recovery tracking:** a clear, auditable record of confirmed recoveries.
- **Dispatch:** the ability to push any case straight to your network operations or fraud team's own system.
- **NL query and API:** plain English answers for your team, plus programmatic access for your systems.

WHO IT IS FOR

- MVNOs without an in-house fraud team
- Smaller carriers and mobile operators
- Revenue assurance and fraud management staff
- Interconnect and roaming teams

2 SUBSCRIPTION TYPES

Every capability described above is available either way. What changes is how you pay for it.

CORE VOLUME

Pay a predictable package. Know your cost before you start.

Billing: one of thirteen fixed monthly packages, billed in advance.

Additional usage: billed per unit at your package's own rate, disclosed up front, so the package that matches your expected volume is always the best value.

Obligations: none beyond the standard subscription terms. No documentation, no agreement to sign.

CORE VALUE

Pay a share of what you recover. Recover nothing, pay nothing.

Billing: a share of the recovered value you document, billed after the fact, never more than 1.5 times what the matching Core Volume package would have cost you. You can move to Core Volume at any time.

Requires: a signed Value Agreement and documentation of every closed case.

Best for: teams who'd rather see results before committing to a subscription.

Both are Signal Core: same scoring, same workflow, same everything above. The only difference is how the bill is worked out.

DEPLOYMENT AND INTEGRATION

Signal Core is a cloud-hosted SaaS platform with role-based access, so there is nothing for your team to host or maintain, which matters most for an MVNO without spare infrastructure budget. Data comes in either through the upload manager or the API, sourced from your existing CDR, billing mediation or interconnect systems. Once your application is approved, a new tenant can be provisioned in minutes, with sandbox demo data available immediately so your team can start evaluating the platform before a single real record is uploaded.

Core Volume and Core Value above are two ways to pay for Signal Core, the same product either way. Signal Score is a different, lighter product: API-only scoring without the case investigation workflow described above, available separately for teams that just want to plug Vantage's risk engine into an existing system.