

PRIIMAL TECHNOLOGIES AS

A Vantage product

WHITE PAPER · PRIIMAL SIGNAL

The MVNO Revenue Assurance Problem

Why Smaller Carriers Carry Full Fraud Exposure With a Fraction of the Detection Infrastructure

Priimal Technologies AS · October 2026 · A Vantage product

ABSTRACT

MVNOs and smaller telecoms carriers face the same fraud typologies as Tier 1 operators. In several key areas, particularly SIM box bypass and subscription fraud, they are structurally more exposed than larger operators due to lighter onboarding controls and greater dependence on host network data that arrives with a processing delay. What smaller operators do not have is the dedicated fraud management infrastructure that major carriers have built over two decades. A single revenue assurance professional at an MVNO running periodic CDR sampling alongside other operational responsibilities cannot detect the multi-account, cross-period patterns that generate the majority of revenue leakage. This is not a headcount problem. It is an architecture problem. This paper describes the specific fraud exposure facing MVNOs, quantifies its financial impact on MVNO margins, and explains why continuous, full-subscriber scoring is the only architecture that addresses it at the scale required.

Document type: Public, Tier 1: no registration required

Audience: MVNO CFOs, revenue assurance leads, MVNO investors and acquirers, telecoms regulators

Product line: Priimal Signal: A Vantage product

The fraud exposure MVNOs are not measuring

The CFCA Global Fraud Loss Survey 2023 placed global telecoms fraud losses at USD 38.95 billion, representing approximately 2.5% of global telecoms revenues. The survey covers all operator types, from global carriers with dedicated fraud management divisions to regional MVNOs with a single revenue assurance generalist. The 2.5% headline rate is an average across that entire spectrum. It does not reveal what smaller operators experience specifically.

Industry evidence suggests that for MVNOs, the effective fraud and leakage rate is higher than the global average. Subscription fraud alone constitutes between 30% and 40% of total fraud losses for many MVNOs, according to industry data published by Vesta in analysis of MVNO payment fraud dynamics. One documented case found that 18% of sign-ups at an MVNO were fraudulent in a single promotional period, generating USD 1.5 million in losses in a single quarter. The MVNO Index publication on MVNO fraud dynamics documents that even modest fraud rates can destabilise MVNO financials given the sector's characteristically narrow margins.

For an MVNO with USD 50 million in annual service revenue, a 5% revenue leakage rate implies USD 2.5 million in annual losses, according to Vesta's 5 to 7% revenue recovery estimate from revenue orchestration implementations. That is not a rounding error on a small operator's income statement. It is the difference between operating profitability and operating loss.

Subscription fraud accounts for 30 to 40% of total fraud losses for many MVNOs. One documented case found 18% of sign-ups in a promotional period were fraudulent, generating USD 1.5 million in losses in a single quarter. For operators with narrow margins, fraud is not a cost of business. It is an existential financial risk.

Why MVNOs are disproportionately exposed

Lighter onboarding controls

MVNOs typically offer simpler, faster activation processes than their host MNO counterparts. The competitive advantage of rapid, frictionless sign-up creates a structural vulnerability: subscription fraud, where synthetic or stolen identities are used to activate services with no intention to pay, exploits exactly the simplicity that MVNOs have deliberately built into their customer acquisition flow. The identity verification steps that a Tier 1 carrier applies at activation are often the steps that MVNOs have removed to compete on customer experience.

The MVNO that has built its growth model on low-friction activation is the same MVNO that is most vulnerable to the synthetic identity attacks that Vesta documents as generating fraud losses of 5 to 7% of revenue for operators without effective controls.

Delayed and batched CDR data

MVNOs receive call detail record data from their host MNO rather than generating it directly from their own network infrastructure. This creates two detection problems that Tier 1 operators do not face. First, CDR delivery is typically batched rather than real-time, meaning that a fraud event is only identifiable after the batch arrives, which may be hours or days after the event occurred. A SIM box operation generating significant daily losses may be active for days before the CDR data needed to detect it reaches the MVNO's revenue assurance system.

Second, the CDR data an MVNO receives from its host reflects billing-rated records rather than raw network events. Mediation failures and rating errors, which may represent a significant share of non-fraud revenue leakage, are invisible in the billing records the MVNO can access. The MVNO cannot see what the host network did not rate; it can only see what was delivered to it. This creates a systematic blind spot in non-fraud leakage detection that is structural to the MVNO operating model.

No dedicated fraud management infrastructure

Tier 1 operators have invested substantially in dedicated fraud management systems over two decades: real-time CDR analytics, SIM behavioural profiling, test call generation for SIM box detection, and revenue assurance platforms from vendors including Subex and Mobileum. These investments were made when those operators had millions of subscribers and the return on investment was immediate.

MVNOs have not made those investments, partly because their subscriber bases are smaller, partly because the capital required is disproportionate to their scale, and partly because the MVNO market has generally assumed that the host MNO's fraud controls offer sufficient downstream protection. They do not: the host MNO's fraud

management is calibrated to protect the host's own revenue, not the MVNO's interconnect arrangements or subscription economics.

Host network interconnect exposure

SIM box fraud, where a bank of SIM cards terminates international calls as local calls to avoid interconnect charges, directly targets the MVNO's interconnect revenue stream. The MVNO is entitled to international termination rates for calls that reach its subscribers from abroad. SIM boxing diverts those calls to local termination rates, extracting the rate differential as fraud revenue. The MVNO loses the interconnect income it was entitled to, and the quality of service delivered to its subscribers may also degrade due to the SIM box routing.

Detection of SIM box fraud requires comparing call patterns at the subscriber level against expected behaviour profiles: high volumes of short-duration calls, consistent call times indicating automated dialling, unusual geographic call-origin distributions. These patterns are detectable in CDR data. They are not detectable by threshold alerts calibrated to individual subscriber usage, because the SIM box operation is specifically calibrated to mimic legitimate high-volume users.

The margin leverage effect

The financial impact of revenue leakage on MVNOs is significantly larger than the gross leakage figure suggests, because of the margin leverage effect. Tier 1 operators typically operate on EBITDA margins of 25 to 40% of service revenue. MVNOs typically operate on margins of 5 to 15% of service revenue, because they pay their host MNO for network access and carry fewer infrastructure assets. A 1% leakage rate on service revenue represents a different financial impact at a 5% margin than at a 30% margin.

For an MVNO with EUR 40 million in annual service revenue and a 10% EBITDA margin, that margin is EUR 4 million. A 2.5% revenue leakage rate (the CFCA global average) implies EUR 1 million in annual losses. That EUR 1 million represents 25% of the operator's EBITDA. At a higher leakage rate, which the evidence suggests is realistic for under-protected MVNOs, the losses can eliminate the margin entirely. Revenue leakage at an MVNO is not a cost of business. At the margin percentages typical of the sector, it is an existential financial risk.

Scenario	Annual service revenue	Leakage rate	Annual leakage	EBITDA margin	EBITDA value	Leakage as % of EBITDA
Conservative	EUR 40 million	2.5%	EUR 1.0 million	10%	EUR 4.0 million	25%
Base case	EUR 40 million	4.0%	EUR 1.6 million	10%	EUR 4.0 million	40%
High exposure	EUR 40 million	6.0%	EUR 2.4 million	10%	EUR 4.0 million	60%

Leakage rates derived from CFCA Global Fraud Loss Survey 2023 (2.5% global average) and MVNO-specific fraud literature. EBITDA margin range of 5 to 15% consistent with published MVNO sector financial benchmarks. Figures are illustrative.

What continuous scoring makes possible

The fraud detection approach that Tier 1 operators use depends on continuous, real-time CDR analytics at the network layer: monitoring every call, every session, every message as it occurs, comparing it in real time against subscriber behaviour profiles and fraud signatures. This architecture is not available to MVNOs: they do not have network-layer access to their subscribers' traffic.

What MVNOs do have is CDR data, billing records, activation records, and payment histories. Scored continuously against cross-subscriber fraud patterns, this data is sufficient to identify SIM box activity through traffic pattern analysis, subscription fraud through activation behaviour profiling, IRSF through termination pattern anomalies, and non-fraud billing leakage through rating exception identification. The data is available. The architecture to score it continuously, across the full subscriber base, simultaneously, is what most MVNOs do not have.

The distinction matters because periodic CDR sampling, which is what most MVNO revenue assurance functions currently do, identifies leakage that has already accumulated. A SIM box operation that is detected in a monthly CDR review has been generating losses for up to thirty days since the last review. At EUR 8 per SIM card per day in

documented interconnect rate differentials, a ten-SIM operation running for thirty days represents EUR 2,400 in losses from a single detection lag. Across an MVNO network with multiple active fraud operations, the monthly detection cycle means paying for a month of fraud before identifying any of it.

Periodic CDR sampling catches fraud after it has accumulated. Continuous scoring identifies it in the current billing cycle. For an MVNO where leakage represents 25 to 60% of EBITDA, the difference between monthly and continuous detection is the difference between managing a cost and losing the margin.

Priimal Signal: A Vantage product

Priimal Signal is an AI-scoring and case management platform for telecoms revenue leakage and fraud analysis, built specifically for MVNOs and smaller carriers. Operators upload their existing CDR exports, billing records, and interconnect settlement data in any format. Vantage scores every record across five fraud flag types: SIM Box, Bypass Fraud, Grey Route, Traffic Pumping, and Roaming Fraud, and returns a prioritised case queue for the revenue assurance team.

For a lean MVNO revenue assurance team where one or two people cover fraud detection alongside other responsibilities, the prioritised queue means the highest-value cases are always visible and actionable without requiring manual CDR sampling or threshold monitoring. Cases include a risk score, confidence level, flag explanation, and the specific pattern signatures that triggered the flag. The workflow supports case investigation notes, status tracking, and field action dispatch.

Available under Core Value: pay a share of documented recovered value only, capped at the flat-rate package equivalent, nothing owed if nothing is recovered. Requires a signed Value Agreement; not self-serve. To discuss a Signal Flash for your operator, contact connect@priimal.com.

Priimal Technologies AS · priimal.com · connect@priimal.com · A Vantage product. Published October 2026. All figures derived from publicly available sources. This document does not constitute legal or investment advice. © 2026 Priimal Technologies AS. All rights reserved.