CASE STUDY

The Silent Drain: Detecting a Slow-Burn Money Laundering Network

How RemitSo's Continuous Transaction Monitoring Uncovered a 90-Day Layering Scheme That Manual Reviews Would Have Missed Entirely

Industry: Money Services Business **Region:** United Kingdom / UAE / Nigeria **Classification:** Confidential

Executive Summary

A UK-based FCA-registered payment institution deployed RemitSo's white-label remittance platform to serve diaspora communities across 25+ corridors. Over a 90-day period, RemitSo's continuous transaction monitoring system tracked subtle, evolving patterns across 23 seemingly unrelated accounts—gradually building a risk profile that revealed a sophisticated layering operation routing £187,000 through the UAE to Nigeria-based shell entities. No single transaction exceeded reporting thresholds. No single alert was conclusive. Only persistent, intelligent monitoring connected the dots.

23	£187K	90 Days	340+	Zero
Linked Accounts Identified	Laundered Funds Intercepted	Monitoring Window	Transactions Analyzed	Manual Alerts Initially

1. The Challenge: When Nothing Looks Wrong

Unlike the dramatic red flags of sanctions evasion or identity fraud, this case presented the most dangerous form of financial crime—**transactions that individually appeared entirely legitimate**. The operator's compliance team conducted regular manual reviews and found nothing unusual. Every customer had passed eKYC, every transaction had a plausible purpose, and no single amount triggered reporting thresholds.

What made this scheme invisible to traditional monitoring:

- **Low-Value Consistency** — Individual transactions ranged between £200 and £800—well below the £1,000 threshold that typically triggers enhanced scrutiny.
- **Varied Timing** — Transactions were spaced 5–12 days apart per account, mimicking genuine family remittance patterns.
- **Diverse Profiles** — Senders included healthcare workers, students, and small business owners—a natural demographic mix for diaspora remittances.
- **Multiple Corridors** — Transactions initially appeared to target different receiving countries before converging on common intermediary accounts in the UAE.

> **The Core Problem:** Manual compliance reviews operate on snapshots—reviewing individual transactions or periodic reports. Sophisticated launderers exploit this by designing patterns that only become visible when monitored **continuously over weeks and months**.

2. How RemitSo’s Monitoring Engine Detected It

Weeks 1–2 | Baseline Behavior Profiling

RemitSo’s **Risk Rule Engine** began building behavioral baselines for all active accounts. During this period, 23 accounts exhibited normal activity—small, periodic transfers to family members in Nigeria, Ghana, and the UAE. Risk-O-Meter scores remained between 10–25 (LOW classification). No alerts were generated.

Weeks 3–5 | Subtle Pattern Divergence

RemitSo’s monitoring engine detected the first deviations from established baselines. While no single trigger was conclusive, the **Risk Rule Engine’s 55+ automated factors** began accumulating micro-indicators:

- **Recipient Convergence** — 8 accounts that previously sent to different recipients in Nigeria began routing funds to a common UAE intermediary account.
- **Amount Escalation** — Average transaction values increased from £280 to £620 across the cluster, while staying below reporting thresholds.
- **Frequency Shift** — Transaction intervals shortened from 10–12 days to 5–7 days for 11 of the 23 accounts.
- **Purpose Code Shift** — 6 accounts changed declared purpose from “Family Support” to “Business Investment” without corresponding profile updates.

Timeline	Accounts Flagged	Avg. Risk Score	Classification
Weeks 1–2	0 of 23	18 / 100	LOW
Weeks 3–5	8 of 23	42 / 100	MEDIUM
Weeks 6–9	19 of 23	67 / 100	HIGH
Weeks 10–13	23 of 23	91 / 100	CRITICAL

3. Deep Investigation: Unmasking the Network

Weeks 6–9 | Network Mapping & Sanction Screening

As risk scores climbed, RemitSo's **Risk Radar** dashboard automatically surfaced the 23 accounts as a connected cluster. The compliance team now had a unified view revealing:

- All 23 sender accounts were routing funds through **3 UAE-based intermediary accounts** that then disbursed to 7 Nigerian beneficiary accounts.
- RemitSo's **Global Sanction Screening Engine** (40,000+ records) identified that one Nigerian beneficiary was a partial match against the **OFAC SDN list**—a company previously linked to trade-based money laundering.
- The **Document Verification Queue** revealed that 5 sender accounts had submitted KYC documents with sequential serial numbers—indicating bulk procurement of identity documents.
- Device fingerprint analysis showed **14 of 23 accounts** had been accessed from just 4 unique devices, with IP addresses concentrated in East London.

Transaction Flow Analysis

Stage	Details	Volume
Placement	23 UK senders → individual small transfers	£187,340 total
Layering	Funds consolidated into 3 UAE intermediary accounts	£182,100 (after fees)
Integration	Disbursed to 7 Nigerian shell company accounts	£176,800 (net)

Weeks 10–13 | Automated Escalation & Account Suspension

By Week 10, all 23 accounts had breached the **Critical threshold (85/100)** on RemitSo's Risk-O-Meter. The system automatically triggered account suspension, froze £12,400 in pending transactions, and escalated all 23 accounts to the Chief Compliance Officer's review queue. The compliance team used RemitSo's **360-degree Customer Profiles** to compile a complete evidentiary package.

4. Response & Regulatory Action

Immediate Containment

- All 23 sender accounts **suspended** and reclassified via RemitSo's **Customer Segments** to "Blocked — AML Investigation."
- 3 UAE intermediary recipient accounts **permanently blacklisted** across the platform.
- £12,400 in pending transactions **frozen**; £174,940 in completed transactions flagged for tracing.
- RemitSo's **High-Risk Country Management** module updated to apply enhanced monitoring to all UAE–Nigeria corridor transfers.

Regulatory Reporting

Using RemitSo's **Transaction Log** and comprehensive audit trail, the compliance team filed coordinated reports with multiple authorities:

- **UK NCA (National Crime Agency)** — Suspicious Activity Reports filed for all 23 accounts with full transaction histories, device fingerprints, and behavioral timeline.
- **FCA Compliance Team** — Proactive notification to the firm's FCA supervisor demonstrating the effectiveness of automated monitoring controls.
- **UAE Financial Intelligence Unit** — Intermediary account details shared for downstream investigation.
- **NFIU Nigeria** — Beneficiary account information and transaction flow analysis shared via international cooperation channels.

Post-Incident Policy Enhancement

The operator implemented five enhanced rules via RemitSo's AML engine: **(1)** Recipient convergence alerts when 3+ senders target the same beneficiary within 30 days. **(2)** Behavioral drift detection comparing current patterns against 60-day baselines. **(3)** Mandatory EDD for cumulative transfers exceeding £3,000 per corridor per rolling 30 days. **(4)** Device-to-account ratio limits of max 3 accounts per device. **(5)** Automated cross-corridor flow analysis for intermediary jurisdiction patterns.

5. Lessons Learned: Why Continuous Monitoring Wins

This case demonstrates that sophisticated money laundering operations are designed to evade point-in-time compliance checks. The perpetrators used authentic identities, legitimate transaction purposes, and carefully calibrated amounts to avoid suspicion. Only through RemitSo's **continuous, behavioral transaction monitoring**—tracking patterns over weeks and months—was the full scope of the network revealed.

1 Behavioral Baselines

Continuous profiling catches drift that snapshots miss.

2 Risk Score Evolution

Dynamic scoring escalated 23 accounts from Low to Critical over 90 days.

3 Network Detection

Risk Radar connected 23 isolated accounts into one cluster.

4 Cross-Corridor Analysis

Intermediary jurisdiction patterns exposed the layering structure.

5 Automated Escalation

System-driven suspension prevented further fund movement.

6 Audit Trail

Complete evidence package enabled coordinated multi-jurisdiction

Final Assessment

The most dangerous financial crimes are not the ones that trigger alarms—they are the ones designed to avoid them entirely. RemitSo's continuous transaction monitoring engine—combining behavioral baselines, dynamic risk scoring, cross-corridor analysis, and unified Risk Radar intelligence—ensures that even the most patient, carefully constructed laundering networks are detected, traced, and reported.

Compliance is not a moment—it is a continuous commitment to vigilance. With RemitSo, that vigilance never sleeps.