RemitSo

CASE STUDY

Stopping a Sanctions Evasion Ring Across Three Continents

How RemitSo's Multi-Layered Compliance Engine Detected a Sanctioned Network Operating Behind Shell Identities in Canada, Turkey & Syria

Industry: Money Services Business **Region:** Canada / Turkey / Syria **Classification:** Confidential

Executive Summary

A licensed Money Services Business (MSB) operating across Canada deployed RemitSo's white-label remittance platform to power its cross-border payment operations. Within 90 days of go-live, RemitSo's compliance engine autonomously detected, flagged, and contained a sophisticated sanctions evasion ring—involving 14 coordinated accounts, stolen identity documents, and structured transactions designed to route funds through Turkey to Syria-linked sanctioned entities.

14	$41K+	40,000+	55+	4 Days
Fraudulent Accounts	Suspicious Funds Frozen	Sanction Records Screened	Risk Rules Activated	Detection to Containment

1. The Incident: When Routine Transfers Signal Danger

Within its first quarter of operation, the MSB was processing over 2,000 monthly transactions across 15 corridors—standard volume for a growing Canadian remittance provider. Operations appeared unremarkable until RemitSo’s **Risk Rule Engine** began surfacing a pattern that no human reviewer would have caught in isolation:

- **Rapid Account Creation** — 14 new accounts registered within a 72-hour window, all originating from the Greater Toronto Area.
- **Transaction Structuring** — Every transaction was calibrated between CAD 900 and CAD 990—systematically below the CAD 1,000 regulatory reporting threshold.
- **Corridor Concentration** — All 14 accounts sent funds exclusively to Turkey, directed to just two recipient accounts.
- **Profile Inconsistencies** — Sender demographics ranged from students to retirees, yet every account declared the identical transaction purpose: “Business Investment.”

> **Assessment:** RemitSo’s automated compliance engine identified this as a potential **sanctions evasion and structuring operation**—a coordinated network using multiple identities to systematically circumvent regulatory thresholds and route funds to sanctioned jurisdictions.

Alert Type	Compliance Layer	Finding
Sanction Hit	Global Screening (40K+ records)	Partial match on OFAC SDN and UK lists — Turkish recipient linked to Syrian national fla
Risk Score Spike	Risk-O-Meter Scoring	All 14 accounts escalated from Low (15/100) to Critical (89/100) within 48 hours
Indicator Cluster	Risk Rule Engine (55+ Factors)	Same-IP registrations, below-threshold structuring, single-corridor concentration, rapid ve
Corridor Flag	High-Risk Country Mgmt	Turkey-to-Syria corridor flagged; beneficiary bank in FATF grey-listed jurisdiction

*RemitSo’s **Risk Radar** dashboard aggregated all indicators into a single unified view, enabling the compliance team to visualize the full scope of the coordinated operation in real time.*

3. Investigation: How RemitSo Unraveled the Scheme

Layer 1 | Real-Time Global Sanction Screening

RemitSo's **Global Sanction Screening Engine** executes automatically on every transaction before funds are released. The engine performs fuzzy matching with configurable thresholds across four internationally recognized databases:

Database	Records Screened	Result
OFAC SDN List (United States)	15,568	PARTIAL MATCH
EU Financial Sanctions	5,030	No Match
UK HM Treasury Sanctions	4,495	PARTIAL MATCH
UN Security Council Consolidated List	875	No Match

The partial matches on OFAC and UK lists revealed that the Turkish recipient shared a name, date of birth, and nationality profile with a Syrian national flagged for **facilitating financial flows to designated entities**. The screening engine automatically escalated the transaction to the compliance review queue.

Layer 2 | Risk Rule Engine — 55+ Automated Risk Factors

Concurrently, RemitSo's **Risk Rule Engine** analyzed all sender profiles against 55+ customizable risk factors. The following triggers were identified across the 14 accounts:

- **Structuring Detection** — All transactions calibrated between CAD 900–990, consistently below the CAD 1,000 reporting threshold. Classic smurfing pattern.
- **Velocity Alert** — 14 accounts created within 72 hours, all initiating transactions within 24 hours of registration.
- **Single-Corridor Concentration** — 100% of transactions from 14 different senders routed to the same country (Turkey) with identical recipients.
- **Device Fingerprint Overlap** — 8 of 14 accounts accessed from the same 3 devices, indicating a single orchestrator.
- **IP Geolocation Mismatch** — Accounts registered from Toronto IPs; 6 subsequently accessed from IPs traced to Gaziantep, Turkey.
- **Profile Inconsistency** — Student-occupation senders declaring "Business Investment" as transaction purpose without supporting documentation.

> **Conclusion:** The Risk Rule Engine confirmed this was not 14 independent customers—it was a single coordinated network using multiple identities to systematically evade transaction monitoring thresholds.

Layer 3 | Integrated AML & KYC Verification

RemitSo's platform integrates **digital eKYC onboarding** with a comprehensive **Document Verification Queue**. Upon risk escalation, the compliance team conducted a thorough examination of all 14 accounts using RemitSo's back-office tools:

- All 14 accounts passed initial eKYC verification—the identity documents were authentic Canadian-issued documents.
- The Document Verification Queue revealed that 9 of 14 passports had been reported stolen within the preceding 6 months.
- Source of Funds documentation was either absent or fabricated—three accounts submitted identical bank statements differing only in the account holder's name.
- RemitSo's KYC Document Categories system flagged missing Proof of Address documentation for 11 of 14 accounts.
- The AML Policy Configuration engine automatically enforced Enhanced Due Diligence (EDD) for transactions exceeding cumulative CAD 3,000 within a 7-day rolling window.

Layer 4 | Risk-O-Meter — Dynamic Customer Risk Scoring

RemitSo's **Risk-O-Meter** assigns a continuously updated risk score to every customer based on their profile attributes, transaction behavior patterns, and screening results. The following table illustrates the score progression for the flagged accounts:

Timeline	Avg. Risk Score	Classification	Primary Trigger
Day 1 (Registration)	15 / 100	LOW	Standard onboarding
Day 2 (1st Transaction)	38 / 100	MEDIUM	Single-corridor + structuring
Day 3 (2nd Transaction)	62 / 100	HIGH	Velocity + sanction partial match
Day 4 (3rd Transaction)	89 / 100	CRITICAL	Device overlap + IP mismatch + EDD

By Day 4, all 14 accounts had breached the **Critical threshold (85/100)**, triggering automatic **account suspension** and escalation to the Chief Compliance Officer's review queue. RemitSo's system had effectively neutralized the operation before any funds reached Syria.

Layer 5 | Risk Radar — 360-Degree Compliance View

RemitSo's **Risk Radar** consolidated all intelligence from the five compliance layers into a single command-center dashboard. At a glance, the compliance team could visualize:

- 14 interconnected accounts identified and flagged as a coordinated cluster
- 2 partial sanction screening matches across OFAC SDN and UK HM Treasury lists
- 47 cumulative risk indicator triggers across the entire account group
- 9 stolen identity documents detected through KYC document verification
- All 14 accounts at CRITICAL risk classification on the Risk-O-Meter
- CAD 41,580 in total suspicious transaction volume frozen and secured

> **Outcome:** The Risk Radar's consolidated view transformed what appeared to be 14 separate low-value transactions into a clearly visible coordinated sanctions evasion network—enabling the compliance team to take decisive action within hours rather than weeks.

4. Containment & Response

Immediate Transaction Containment

- All pending transactions totaling **CAD 41,580** to the two Turkish recipient accounts were **frozen instantly**.
- All 14 sender accounts were **suspended** pending formal investigation.
- Both Turkish recipient accounts were **permanently blacklisted** across the platform.
- RemitSo's **Customer Segments** feature reclassified all 14 accounts from "Standard" to "Blocked — Sanctions Risk."

Regulatory Reporting & Law Enforcement Coordination

Using RemitSo's **Transaction Log** and **360-degree Customer Profiles**, the compliance team filed reports with:

- **FINTRAC (Canada)** — STRs filed for all 14 accounts with full transaction histories, device fingerprints, and IP logs.
- **RCMP Financial Crime Unit** — Evidence of stolen identity documents shared, initiating criminal investigation.
- **OFAC (United States)** — Sanctions match intelligence forwarded for cross-border information sharing.
- **MASAK (Turkey)** — Recipient account details shared for investigation of the intermediary network.

Post-Incident AML Policy Enhancement

The MSB implemented five enhanced rules via RemitSo's configurable AML engine: **(1)** Structuring threshold reduced to CAD 750 for Turkey. **(2)** Mandatory EDD for accounts transacting within 24 hrs of registration. **(3)** Video verification for scores above 60/100. **(4)** Max 2 accounts per device fingerprint. **(5)** Source-of-funds docs for FATF grey-listed corridors.

5. Lessons Learned: Why Layered Compliance Wins

This case demonstrates that no single compliance check is sufficient against sophisticated threat actors. The perpetrators passed eKYC using authentic (stolen) documents, structured amounts to avoid regulatory thresholds, and exploited intermediary jurisdictions to obscure fund flows. Only through RemitSo's **multi-layered compliance architecture** was the scheme detected and neutralized within four days.

1

Sanction Screening

Real-time screening against 40K+ global records caught the

2

Risk Rule Engine

55+ automated factors detected structuring and velocity patterns.

3

KYC Integration

Document verification queue exposed 9 stolen identity documents.

4

Risk-O-Meter

Dynamic scoring escalated all accounts from Low to Critical in 4 days.

5

Risk Radar

Unified dashboard connected all data points for the compliance team.

6

AML Policies

Configurable rules enabled real-time policy tightening post-incident.

Final Assessment

Sanctions evasion networks are growing in sophistication—leveraging stolen identities, structured transactions, and intermediary jurisdictions to obscure their true intent. RemitSo's layered compliance engine—combining real-time sanction screening, intelligent risk scoring, automated AML policy enforcement, and a unified Risk Radar—ensures that even the most carefully disguised operations are detected, contained, and reported.

Compliance is not a checkbox—it is an ongoing commitment to financial integrity.
With RemitSo, that commitment is always active.