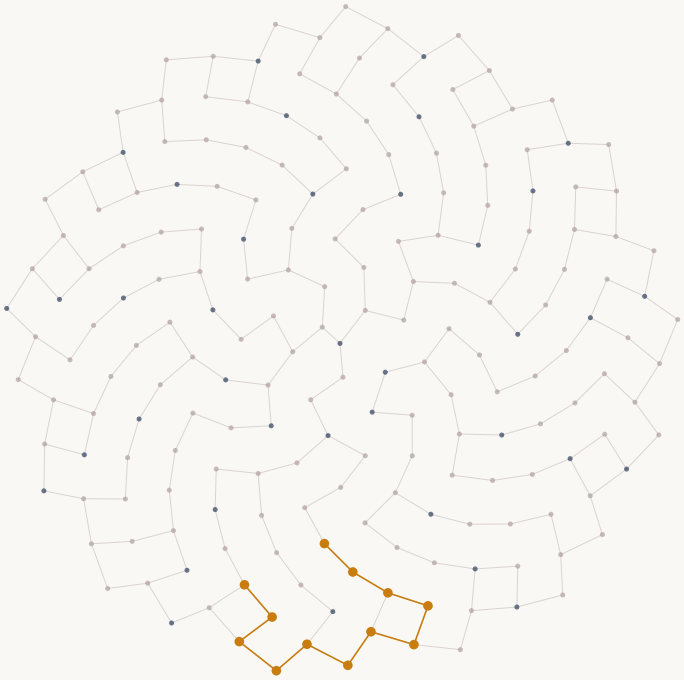
A SAYARI SANCTIONS BLOG . NOVEMBER 2024 . SAYARI ANALYST TEAM



Russian Sanctions Evasion Has Gone Sectoral

Seafood, shipbuilding, and the limits of watchlist screening in detecting complex corporate networks behind sanctions violations.

By Sayari Analyst Team . Published November 2024 . sayari.com

SANCTIONS

Russian Sanctions Evasion Has Gone Sectoral

By Sayari Analyst Team · Published November 2024

Seafood, shipbuilding, and the limits of watchlist screening in detecting complex corporate networks behind sanctions violations.

Most compliance professionals assume that Russian sanctions evasion follows a predictable pattern: shell companies obscure beneficial ownership, OFAC watchlists catch the obvious violators, and trade screens flag sanctioned commodities at the border. But that model is becoming obsolete. The real risk today isn't in the sanctioned parties you're missing-it's in the legitimate trade flows you're not interrogating. Russian actors have stopped relying on crude list evasion and shifted to a fundamentally different strategy: weaponizing legal corporate networks to move money and materials through open markets. This shift has spawned new typologies that operate entirely outside traditional sanctions screening frameworks, and detecting them requires abandoning commodity-level monitoring in favor of beneficial ownership and network analysis.

Cash-for-Seafood: When Legal Trade Carries Illegal Cash

The original post "Beyond Cash-for-Gold" identified three distinct Russian sanctions evasion typologies that were barely discussed in compliance circles until recently. The first, cash-for-gold, remains the baseline-Russian exporters sell physical gold to international buyers while simultaneously receiving cash transfers that flow back into the Russian economy, circumventing SWIFT restrictions and asset freeze requirements. But Russia's sanctions architects have evolved far beyond gold. Two new typologies have emerged with striking regularity: cash-for-seafood and shipbuilding parts diversion. Cash-for-seafood operates through a counterintuitive reversal of normal goods-for-cash transactions. Japanese seafood importers purchased over one billion dollars in legitimate Russian seafood in 2022, yet parallel cash transfers-physical banknotes in some cases-flowed back to Russian counterparts through intermediaries that had no documented connection to the seafood supply chain. The goods moved one direction; the money moved another. Sayari analysts tracing these flows discovered that the corporate networks linking Japanese importers to Russian receivers included shell entities registered in jurisdictions with weak beneficial ownership disclosure requirements, obscuring the true economic interest of the money transfers. Similarly, Dutch investigative reporting uncovered shipbuilding components flowing from legitimate manufacturers through opacity-prone intermediaries to Russian end beneficiaries, violating EU export control frameworks while remaining invisible to transaction-level monitoring.

Why Traditional Screening Misses These Typologies

What makes these typologies so dangerous is that they exploit a critical gap between how compliance teams screen trades and how sanctions architecture actually works. Traditional trade-based money laundering detection focuses on commodity profiles-is the price reasonable? Is the volume typical? Are the goods listed on restricted commodity lists? But these new Russian evasion schemes move entirely legal commodities through entirely legal companies. A billion-dollar seafood import business is legitimate commerce; there is nothing inherently suspect about Japanese companies sourcing Russian fish. The red flag emerges only when beneficial ownership analysis reveals that corporate networks financing those imports include entities controlled by individuals or organizations with Russian government connections or documented ties to entities subject to sectoral sanctions. Watchlist screening cannot detect this because the importing companies themselves are not on the SDN list and the seafood is not a restricted commodity. The evasion works precisely because it sits within the compliance blind spot between commodity screening and network due diligence.

The Corporate Network Problem Compounds Detection Gaps

The corporate network problem deepens when intermediaries intentionally fragment information across jurisdictions. A Japanese importer might contract with a Singapore-registered trading company, which then sources from a British invoice trader, which connects to a Dutch shipper, which finally touches the Russian supplier. At each stage, a single transaction appears normal-a trader buying from a supplier, a shipper arranging transport, an importer receiving goods. But across the full network, beneficial ownership remains obscured. Traditional sanctions screening systems check each entity at the transaction point; they do not reconstruct the full chain of corporate control. A legitimate-appearing Japanese company passes OFAC checks because it is genuinely a legitimate business. The sanctionable activity-moving value to Russian actors-happens in parallel through a separate payment channel that nominally relates to the seafood trade but operates independently from it. The compliance officer reviewing the Japanese importer's files sees a purchase order, an invoice, a bill of lading, and a payment from a known bank. What they don't see is the beneficial ownership diagram showing that the payment ultimately serves Russian interests.

From Cash-for-Gold to Sectoral Evasion: What Detection Requires

Detecting these typologies requires a fundamental shift in detection methodology. Commodity-level screening and OFAC list matching remain necessary but insufficient. Compliance teams and law enforcement must map the beneficial ownership structures of all parties in a supply chain, not just the direct counterparties. This means cross-referencing corporate registry data across multiple jurisdictions, analyzing unusual payment patterns that diverge from normal trade finance, and identifying networks where multiple entities share common owners, addresses, or registered agents-even across countries. Japan's Ministry of Economy, Trade and Industry and the Financial Services Agency have begun requiring banks to conduct full-chain beneficial ownership analysis on imports from Russia, but most jurisdictions have not caught up. FinCEN's advisory guidance on trade-based money laundering remains focused on individual transaction red flags rather than network-level indicators. Effective detection also requires closer coordination between customs authorities, central banks, and financial intelligence units to share network information that a single institution cannot access.

The evolution from cash-for-gold to sectoral typologies signals that Russian sanctions evasion has matured into a sophisticated discipline that exploits the architecture of global trade finance itself. Stopping it demands more than better watchlists or commodity monitoring. It requires the ability to see across corporate networks, across jurisdictions, and across time. Teams responsible for financial crime investigations and sanctions compliance now operate in an environment where legitimate imports genuinely do involve billions of dollars flowing from Japan to Russia, and distinguishing between lawful commerce and sanctions evasion turns on questions of beneficial ownership that traditional screening systems cannot answer. This is where network-level due diligence becomes not a compliance enhancement but a regulatory necessity.

Sayari's platform was built to answer exactly these questions by mapping corporate networks and tracing beneficial ownership across borders. The intelligence required to detect cash-for-seafood flows or shipbuilding diversion schemes sits in the intersection of trade data, corporate registries, and ownership information that Sayari integrates in real time. For law enforcement and regulatory teams managing Russian sanctions portfolios, the path forward is clear: shift from entity-level screening to network-level investigation. If you're responsible for catching sanctions evasion in the era of sectoral typologies, request a demo to see how network mapping changes what you can detect.

Please visit sayari.com to learn more.

This blog is for informational purposes and isn't intended to be legal advice.