



Russian Sanctions at Three Years: The Evasion Playbook Today

Shadow fleets, gold-for-cash corridors, and third-country transshipment have replaced simple asset concealment.

Here's what the Russian sanctions evasion playbook looks like now.

SANCTIONS

Russian Sanctions at Three Years: The Evasion Playbook Today

By Sayari Analyst Team · Published May 2025

Shadow fleets, gold-for-cash corridors, and third-country transshipment have replaced simple asset concealment. Here's what the Russian sanctions evasion playbook looks like now.

When OFAC, OFSI, and the EU began their sanctions campaign in February 2022, name-list matching was sufficient. Three years later, that playbook is obsolete.

Russia's sanctions evasion infrastructure has professionalized across three axes: commodity routing, shell company layering, and third-country transshipment. The structures don't carry Russian names. They operate through Turkish, Emirati, Indian, and Chinese intermediaries with no SDN List exposure. They move physical commodities—crude oil, gold, dual-use machinery—through legitimate trade channels, obscured by layers of corporate registration. Legacy sanctions screening catches zero of this architecture.

The First-Generation Evasion Toolbox: What the 2022 Playbook Looked Like

In the weeks after February 24, 2022, Russian sanctions evasion was straightforward. Oligarchs moved yachts from European ports. Wealth management accounts came into focus. Front companies held assets offshore. OFAC's SDN List grew to include state entities, oligarchs, and business associates. Many shell companies carried Russian names or obvious markers. By late 2022, low-hanging fruit was gone and what remained required network analysis.

The Shadow Fleet and Commodity Routing: How Evasion Scaled

The turning point came in 2023. Russian crude oil—a critical source of foreign exchange for the state—faced a price cap under the EU ban. Europe's refineries closed to Russian supply. So Russia built a new logistics network outside Western regulatory view.

By late 2024, the shadow fleet comprised 500 to 600 vessels operating outside Western oversight. These ships moved Russian crude to India, China, and Turkey under false origin documentation. OFAC responded with systematic shadow fleet designations in 2024, but networks adapted faster than designations accumulated.

The shadow fleet's operational structure reveals the depth of sanctions evasion architecture. These vessels are typically 15 to 30 years old—above the age threshold that triggers automatic insurability scrutiny from major Western brokers, but young enough for extended operational life. Registration happens through flag registries in Gabon, Palau, Mongolia, and Togo, jurisdictions offering minimal transparency into beneficial ownership and limited enforcement of international maritime standards. Insurance underwriting occurs through non-traditional brokers in Dubai, Istanbul, and Singapore, firms that accept substantially higher risk in exchange for access to disabled shipping sanctions. Through 2023 and early 2024, OFAC designated over 180 shadow fleet vessels individually, yet the fleet continued growing because new vessels entered service faster than enforcement could accumulate targets. The designations followed a pattern: once a vessel reached 15 designations or flagged as Russian-linked, operators simply reregistered the hull under a new name and flag. The operational economics remain favorable because freight rates for Russian oil had widened the margin sufficient to absorb loss of individual vessels.

Gold emerged as a crucial corridor. Russian state gold sales faced EU restrictions, so gold moved through Dubai, Istanbul, Yerevan, and Baku. Turkish and Emirati intermediaries purchased Russian gold and resold it without export documentation. Unlike crude oil, gold is fungible and requires minimal transshipment infrastructure, making detection nearly impossible. The corridors relied on legitimate banking relationships and trade finance instruments—letters of credit, title transfers—that appeared unremarkable when screened in isolation.

These systems didn't require Russian SDN designations. They required logistics networks, ship registers, insurance brokers, and front companies—all legitimate businesses with no sanctions exposure.

Third-Country Transshipment and Trade-Based Money Laundering

Turkey, the UAE, Armenia, Georgia, and Kazakhstan became primary corridors for dual-use goods entering Russia. Turkey's geographic proximity, weak border enforcement, and robust banking infrastructure made it the natural hub for machinery, semiconductors, and electronics. Goods entered Turkey legally then moved across the land border via Georgia, Azerbaijan, and Armenia. Dubai serves a parallel function for liquid commodities and precious metals, with Free Trade Zones permitting goods to be held and transshipped with minimal disclosure of final destination.

Trade-based money laundering through these corridors involves deliberate pricing distortion. Over-invoicing-exporting goods at 30 to 50 percent above market rate-creates implicit value transfer favoring the Russian importer. Under-invoicing directs value outward when Russian exports flow through the transshipment hub. False commodity descriptions allow sanctioned goods to travel under commodity codes that don't trigger alerts: industrial machinery listed as scrap metal, semiconductors as replacement parts. These transactions appear legitimate because documentation maintains internal consistency.

Networks executing this weren't staffed by designated individuals. They were shell companies registered in Hong Kong, Cyprus, and the UAE, with beneficial ownership concealed through layered intermediates. A Turkish trading company importing semiconductors appears standard; the beneficial owner-a designated Russian national-may be concealed through three layers of Hong Kong intermediaries, each holding 30-40 percent stakes, with remaining ownership split among nominees. SDN screening sees only the Turkish company. Detecting the Russian connection requires ownership analysis across corporate registries.

What Defensible Sanctions Monitoring Requires Now

The gap between legacy sanctions screening and 2024-2025 evasion methods has created enforcement risk. OFAC penalties surged 417 percent in the first half of 2025. Financial services firms accounted for over 60 percent of penalties, with substantial settlements among banks operating correspondent relationships in transshipment jurisdictions. Violations ranged from willful evasion to negligent failure to detect beneficial ownership links to designated entities. A single pattern violation-multiple transactions with transshipment hubs sharing ownership networks with designated persons-has resulted in settlements exceeding \$200 million.

Defensible monitoring requires four capabilities: corporate ownership analysis across 250+ jurisdictions; trade flow mapping; vessel tracking and maritime data integration; and financial crime data connecting corporate records to sanctions risk.

Banks with exposure to Turkey, the UAE, Armenia, and other transshipment hubs face concentrated sanctions risk. A single correspondent relationship with a Turkish bank creates implicit exposure to every transaction that bank processes. If the correspondent permitted a shell company with Russian beneficial ownership to maintain accounts conducting trade finance, the originating bank effectively financed sanctions evasion. Correspondent banking liability is strict-the originating bank cannot claim reliance on the correspondent's due diligence if the correspondent's customer violated sanctions.

If your compliance team relies on SDN screening and address matching, you lack visibility into how Russia sanctions evasion actually works. The 2022 playbook is obsolete. The 2024 playbook requires different monitoring entirely.

Learn more about how Sayari helps financial crime teams uncover beneficial ownership networks and map trade-based evasion schemes at Sayari's financial crime solutions.

Please visit sayari.com to learn more.

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