Contents

Maritime Sanctions Red Flags: A Field Guide for the New Compliance Officer

Prepared August 2026. This is a snapshot, not a static reference: the vendor landscape in maritime risk data consolidates constantly (Kpler's absorption of MarineTraffic and FleetMon is a recent example), and OFAC, OFSI, and the EU all revise their maritime guidance every year or two. Confirm current features and access before relying on anything below for a live decision.

A company with maritime exposure can meet sanctions risk from several directions at once: as a charterer, a cargo owner, a financier, an insurer, a port service provider, or simply a counterparty to any of these. The tactics used to move sanctioned cargo around that exposure aren't random. Regulators have been cataloguing them since the U.S. Treasury, State Department, and Coast Guard issued their first joint global advisory in May 2020, and have refreshed that catalogue repeatedly since as evasion networks around Russian, Iranian, and North Korean trade have adapted. What follows is organized in two parts: first, the red flags themselves and how the industry generally responds to each; second, every data source, platform, and service named in that first part, regrouped by what kind of solution it is, with a plain synopsis of what it does and how well.

Nothing below is a substitute for judgment. These tools narrow down where to look. They don't make the call for you.

Part 1: The Red Flags, and How the Industry Responds

1. AIS manipulation, spoofing, and going dark

Every large vessel carries an Automatic Identification System (AIS) transponder that broadcasts its position, speed, heading, name, and a unique identifier called an MMSI number. Deceptive operators manipulate this in three main ways: switching the transponder off for a period (commonly called "going dark"), transmitting a false position (spoofing), or broadcasting another vessel's identity entirely. OFAC's April 2025 advisory on Iranian oil and the Price Cap Coalition's October 2024 update both single this out as a defining shadow-fleet tactic, and October 2024's compliance guidance from OFAC includes a worked example of a port agent discovering, through AIS review, that a vessel could not physically have loaded where its certificate of origin claimed.

Compliance teams generally don't trust AIS alone to answer the question of where a vessel actually was. They flag AIS gaps above a chosen length in known high-risk waters, then cross-check that gap against position data that doesn't depend on the vessel's own self-reporting. Windward, Pole Star Global's PurpleTRAC, and Lloyd's List Intelligence's Seasearcher all build automated gap detection and "dark activity" scoring into their vessel screening, layered on top of terrestrial and satellite AIS feeds. For independent verification, HawkEye 360 uses a cluster of small satellites to geolocate a vessel's other radio emissions, such as its marine radar or VHF radio, regardless of what its AIS is or isn't broadcasting, while radar-imaging satellites from companies including ICEYE and Capella Space, and optical imagery from providers such as BlackSky, can visually confirm a vessel's position or catch a ship-to-ship transfer happening during a dark period. Spire Global runs its own satellite AIS network and RF-based dark-vessel detection alongside it.

This combination is genuinely useful for narrowing a wide ocean down to a specific anchorage or port during a known gap, but it stays probabilistic. Detection-rate claims from any of these vendors are marketing figures, not independently audited numbers, and none of them can prove intent behind a gap: weather, remote areas with no terrestrial AIS coverage, and simple equipment failure all produce identical-looking gaps. A human analyst still has to weigh the pattern.

2. Ship-to-ship transfers used to obscure origin

A ship-to-ship (STS) transfer moves cargo between two vessels at sea, sometimes at a recognized STS zone and sometimes in open ocean chosen specifically because nobody's watching. There are entirely legitimate reasons for one (draft restrictions, weather, lightering into a smaller vessel for port access), but it's also a classic laundering step: sanctioned-origin cargo loaded onto a second, cleaner-looking tanker so the eventual buyer, and that buyer's bank, never see a direct link to the sanctioned origin. Both the Price Cap Coalition's October 2024 update and OFAC's own scenario guidance from the same month treat repeated STS activity, particularly several transfers per shipment, as one of the clearer indicators of evasion.

The standard response is to maintain a running list of known STS hotspots, Malaysia's Eastern Outer Port Limits near Singapore, waters off Fujairah, and parts of the Eastern Mediterranean near Syria come up repeatedly in enforcement actions, and to treat any STS event involving a vessel with other risk indicators (age, ownership opacity, a recent flag change) as grounds to document cargo origin before the counterparty is onboarded. The same integrated platforms named above detect STS events by watching two vessels' AIS

tracks converge and slow to a stop, and increasingly layer in SAR satellite imagery to confirm a physical transfer even through an AIS gap. Vortexa and Kpler go a step further, trying to attach an actual cargo grade and volume to the transfer, which matters because a compliance officer usually needs to know not just that an STS happened but what changed hands.

Detecting that an STS occurred is fairly reliable now, as long as at least one of the two vessels keeps broadcasting. Detecting one where both vessels go dark for the transfer itself depends on the imagery and RF layer, and satellite revisit rates are still nowhere near continuous AIS coverage.

3. Flag hopping, reflagging, and false or fraudulent flagging

A vessel's flag state is supposed to be a stable fact, but shadow-fleet vessels frequently change registry, sometimes mid-voyage, and sometimes to a flag that has already refused or revoked them, in which case the vessel is sailing under no legitimate flag at all. The Kyiv School of Economics Institute's tracking of Russia's shadow fleet has documented flags shifting first to smaller, high-risk registries and then, after sanctions designation, consolidating under the Russian flag itself. Panama, grey-listed under the Paris MOU port state control regime, is the single most common flag among newly identified shadow tankers in KSE's data. Frequent registry changes, and registration with a flag known to apply little due diligence, are both treated as red flags in their own right.

Verifying a vessel's actual, current flag, and its flag history, against an independent source rather than the certificate the vessel itself presents is the basic response. Equasis carries flag history as part of its free ship record, and the commercial platforms fold flag changes and flag-state quality into their overall risk scoring. Paris MOU's flag performance list (white, grey, and black, based on detention rates) is a useful independent input for judging whether a given flag state is one that actually enforces standards. This is one of the more straightforward checks in the whole set: the data is public, and a flag either is or isn't currently valid. The harder judgment call is how much weight to put on a legitimate flag state that simply has weak oversight capacity, which is a spectrum rather than a yes-or-no answer.

4. Falsified or inconsistent cargo documentation

Bills of lading stating a false country of origin, certificates of origin that don't match a vessel's actual voyage history, and insurance certificates naming insurers that don't in fact provide the claimed cover are all documented tactics in OFAC's guidance. The October 2024 compliance communiqué's own example involves a certificate of origin claiming Omani loading that AIS review and ship's logs showed was physically impossible. Legal commentary on OFAC's April 2025 advisory notes an additional, more technical check available to enforcement: crude oil carries a chemical signature that can identify its country of origin independent of whatever the paperwork says.

The practical response most compliance officers can actually run is a cross-check, not a lab test: pull the vessel's independently sourced voyage history and compare it against what the bill of lading and certificate of origin claim about loading location and date. Pole Star's PurpleTRAC includes a bill-of-lading and goods-description screening module, marketed as DUG Screening, that checks cargo descriptions and discharge countries against restricted-goods and sanctioned-region lists. Beyond that, there isn't a mature, independent commercial product for verifying whether a given paper document is authentic the way there is for vessel tracking. The workable fix is the voyage-history cross-check described above, pulling records from Sea-web, Equasis, or a Seasearcher or PurpleTRAC report, rather than document forensics.

5. Layered and opaque vessel ownership

A single-ship shell company, newly formed, registered in a low-transparency jurisdiction, and disclosing no beneficial owner, is one of the most consistent features across shadow-fleet vessels. KSE Institute's research on newly deployed Russian shadow tankers repeatedly finds ownership parked in Seychelles, Mauritius, and the Marshall Islands behind companies that manage exactly one vessel each. OFAC's April 2025 guidance goes further, warning that some of the individuals behind these structures have no public profile, no disclosed source of wealth, and in some cases fraudulent or citizenship-by-investment passports. The legal hook that turns this from a reputational concern into a compliance requirement is the so-called 50% Rule: an entity owned 50% or more by a sanctioned party is treated as sanctioned itself, whether or not it's separately listed.

Addressing this means tracing ownership through however many corporate layers it takes to reach an actual person or state, not stopping at the registered owner named on a certificate. Sayari is built specifically for multi-hop ownership resolution and explicitly markets 50% Rule calculation across corporate structures, drawing on primary-source registry filings rather than self-reported data. On the maritime side specifically, both S&P Global's Sea-web and Lloyd's List's Seasearcher advertise multiple levels of vessel ownership (up to seven, in both cases), which matters because shipping ownership structures often run deeper than a general-purpose KYC tool expects. Dun & Bradstreet and LSEG's World-Check also show up as ownership-data sources inside several of the maritime platforms.

This is genuinely one of the hardest problems in the set, because defeating exactly this kind of tracing is the entire point of the structure. Jurisdictions with weak corporate registries, which is not a coincidence given where a lot of these vessels are registered, simply don't publish the underlying ownership data for any tool to find. Ownership tracing is only as good as the source registries feeding it.

6. The shadow fleet as an aggregate risk profile

Kpler's own published methodology draws a useful distinction worth keeping straight: the "shadow fleet" is the broad category of vessels engaged in sanctions evasion or illicit trade, while the "dark fleet" is the subset that actively conceals its movements through AIS manipulation. Characteristic features, drawn out repeatedly in KSE Institute's monthly tracking, include vessels well over fifteen years old, single-ship ownership through opaque holding companies, non-traditional insurance, frequent flag changes, and a trading history confined to sanctioned or high-risk cargo.

Rather than screening a single vessel against a single list and stopping there, compliance teams increasingly build a running risk score that blends several of these individually weak signals into one picture. The logic, echoed across the industry and set out fairly explicitly in Kpler's published risk-tree methodology, is that vessels which eventually get sanctioned typically showed several of these behavioral signals well before designation. Windward, Pole Star, Lloyd's List Seasearcher, and Kpler all maintain a version of a shadow-fleet or dark-fleet list as a standing filter inside their platforms. Two free, independently produced trackers are worth knowing specifically because neither is selling a compliance subscription: the Kyiv School of Economics Institute's monthly Russian Shadow Fleet Tracker, and United Against Nuclear Iran's Tanker Tracker, built on its MINERVA vessel-behavior system, which covers the Iranian side of the trade. Both are genuinely useful for understanding the current scale and shape of the problem and for spot-checking an individual vessel name, though neither is built or warranted as a transactional compliance product wired into day-to-day onboarding.

7. Insurance gaps and P&I irregularities

Legitimate deep-sea tankers carry Protection & Indemnity (P&I) cover, historically dominated by the twelve mutual clubs of the International Group of P&I Clubs, which together cover the large majority of the world's ocean-going tonnage. Shadow-fleet vessels increasingly carry no verifiable cover at all, or cover from small, newly formed insurers, some specific domestic Russian insurers appear repeatedly in KSE Institute's data, that couldn't actually pay out on a major claim. That gap is an environmental and financial risk in its own right, on top of the sanctions exposure it signals.

The response is to verify that a vessel's claimed insurer is a real, adequately capitalized underwriter rather than just a name typed onto a certificate, and to treat International Group membership, or the absence of it, as one input into the broader risk picture rather than a standalone pass or fail. The International Group's own site confirms which of its twelve member clubs cover a given owner, Equasis carries insurer-of-record data as part of its free ship profile, and the commercial maritime platforms fold insurance status into their overall vessel risk score. This category is more binary and easier to verify than ownership tracing, since IG membership data is public and unambiguous, but confirming that a non-IG insurer is real and solvent, rather than a shell set up specifically to paper over a shadow-fleet vessel, requires the same kind of corporate-registry digging described under ownership above.

8. Substandard vessels and port state control history

Age, poor maintenance, detentions and deficiencies logged during port state control (PSC) inspections, and a pattern of moving away from the more rigorous classification societies that belong to the International Association of Classification Societies (IACS) toward smaller, non-IACS class societies, are all recognized proxies for a vessel cutting corners. In practice, sanctions evaders and genuinely substandard operators overlap heavily, since staying under the radar and avoiding a rigorous survey tend to go together.

Pulling PSC detention and deficiency history, and confirming current classification status, should be a routine part of vetting rather than a separate safety exercise. THETIS, the port state control database for the Paris MOU region, and the equivalent regional MOU databases elsewhere, publish inspection and detention records. IACS's own "Vessels in Class" tool confirms whether a vessel's classification society is actually an IACS member in good standing, and Equasis pulls PSC history, class status, and flag-state performance ratings together into one free record. These are solid source-of-record data for the narrow question of whether a vessel has been detained or holds current class, but none of them assess sanctions risk directly. They complement the tools above rather than replace them.

9. High-risk ports, anchorages, and dark port calls

Certain anchorages and stretches of water recur constantly in enforcement actions and advisories as STS and transshipment hubs, Malaysia, Fujairah, and parts of the Eastern Mediterranean among them. A "dark port call," where an AIS gap lines up neatly with the time it would have taken a vessel to reach and load or discharge at a sanctioned port, is one of the more specific red flags OFAC's guidance names directly.

Maintaining and regularly updating an internal list of high-risk ports and anchorages, informed by current advisories rather than a static list frozen at some earlier point, and treating any AIS gap long enough to reach one of them as grounds for investigation, is the standard practice. The same behavioral-analytics platforms already discussed build port-call and anchorage risk directly into their alerting, and Kpler's published risk-tree write-up is a reasonably clear public description of how one vendor actually weights geography into a score, useful if the goal is to understand or replicate the logic internally rather than rely entirely on a vendor's black box. Geography-based flagging inherits every limitation already noted for AIS-gap and STS detection, since it depends on the same underlying position data.

10. Cargo-level red flags and price-cap evasion

Beyond questions of origin, compliance with the Russian oil price cap has become its own distinct exercise: certifying that a cargo was purchased at or below the applicable cap and watching for signs the price was misstated, such as an invoiced value that's implausibly low relative to freight and insurance costs. Cargo "blending," mixing sanctioned-origin product with unsanctioned product before sale to obscure its origin, is a related and increasingly documented tactic. Vortexa's own analysis has flagged a further wrinkle worth knowing about: "zombie tankers" that reuse a scrapped vessel's identity, allowing sanctioned cargo to pass through screening tied to a hull that no longer physically exists.

The Price Cap Coalition's guidance sets out a documentation-and-attestation model rather than direct chemical verification for every cargo. The counterparty certifies the price paid, and the compliance officer keeps that attestation on file alongside freight cost data and market benchmarks to sanity-check it, since cargo testing in the lab sense is realistically reserved for enforcement agencies and high-value investigations rather than routine due diligence. Vortexa and Kpler both publish grade-level cargo and freight-rate data useful as an external benchmark for whether an attested price looks plausible. This kind of benchmarking is a genuinely useful sanity check, but it flags cargoes worth harder questions rather than proving compliance or evasion on its own.

11. The baseline: sanctions list and counterparty screening

Underneath everything above sits the more basic requirement that still catches the majority of real designations: checking the vessel, its registered owner, its manager, its charterer, and its ultimate beneficial owners against the actual sanctions lists, OFAC's SDN and Consolidated Non-SDN lists, the EU's consolidated list, the UK's list, and the UN's, every time a new counterparty is onboarded, and again on a recurring schedule after that, since a clean name today can be designated tomorrow.

Automating list screening, rather than checking each name by hand, matters for speed and for producing a defensible audit trail, and re-screening the existing counterparty book on a schedule rather than only at onboarding closes an otherwise obvious gap. OFAC's own free Sanctions List Search tool and downloadable list files are the primary source for the U.S. programs and cost nothing to use directly; the EU Sanctions Map serves the same purpose for EU measures. OpenSanctions aggregates several hundred official lists, sanctions and otherwise, into one open database and API, free for non-commercial use, and is worth knowing as a genuinely open alternative or supplement to the commercial vendors, though commercial use still requires a data license. On the commercial side, LSEG's World-Check and Dow Jones Risk & Compliance are the two most widely used curated screening datasets across financial-crime compliance generally, and both appear integrated into several of the maritime-specific platforms discussed above rather than existing purely as standalone maritime products.

Pure name-matching is close to a solved problem, in the sense that these tools reliably catch known names. But the entire point of most of the tactics in sections 1 through 6 is to keep the actual controlling parties off the list in the first place, so list screening alone catches only the fraction of shadow-fleet exposure that's already been formally designated.

Part 2: The Same Tools, Organized by Type of Solution

Every synopsis below reflects the provider's own public description of the product, alongside independent reporting where it exists. Detection rates, coverage percentages, and similar performance figures quoted by any vendor are that vendor's own claim, not an independently audited benchmark; treat them as marketing until verified against your own experience.

A. Regulatory guidance and reference documents (free, public)

Guidance to Address Illicit Shipping and Sanctions Evasion Practices (May 14, 2020) — U.S. Departments of Treasury and State, and U.S. Coast Guard
https://ofac.treasury.gov/recent-actions/20200514
The foundational tri-agency advisory that first set out deceptive shipping practices as a named compliance category, with a focus on Iran, North Korea, and Syria. Every later maritime advisory builds on this one.

Updated Price Cap Coalition Advisory for the Maritime Oil Industry and Related Sectors (October 21, 2024) — OFAC, on behalf of the Price Cap Coalition (G7, EU, Australia, New Zealand)
https://ofac.treasury.gov/media/933506/download?inline=
Updates the Coalition's original October 2023 advisory with sharper detail on shadow-fleet AIS manipulation, STS activity, and flag behavior. The most current single reference for the Russia-focused side of the picture.

OFAC Compliance Communiqué: Sanctions Compliance Guidance for the Maritime Shipping Industry (October 31, 2024) — OFAC
https://ofac.treasury.gov/media/933556/download?inline=
Scenario-based guidance walking through realistic fact patterns (including the falsified certificate of origin example referenced above), aimed at brokers, insurers, ship managers, and port authorities.

Advisory for Shipping and Maritime Stakeholders on Detecting and Mitigating Iranian Oil Sanctions Evasion (April 16, 2025) — OFAC
https://ofac.treasury.gov/media/934236/download
An update to the September 2019 Iran-specific advisory, issued alongside the "maximum pressure" policy directive on Iran. The most detailed current source on shell-company networks, oil brokers, and insurance red flags tied specifically to Iranian crude.

Quint-Seal Compliance Note: Know Your Cargo (December 11, 2023) — DOJ, Commerce/BIS, DHS/HSI, State/DDTC, and OFAC, jointly
https://ofac.treasury.gov/recent-actions/20231211_33
A five-agency note aimed more broadly at cargo transport (not maritime alone), reiterating red flags and setting expectations for compliance programs across the wider trade and logistics chain.

OFSI Maritime Shipping Guidance (refreshed February/March 2024) — HM Treasury's Office of Financial Sanctions Implementation
https://ofsi.blog.gov.uk/2024/02/28/ofsi-refreshes-its-guidance-for-the-maritime-sector/
The announcement and entry point for OFSI's UK-specific maritime guidance, covering illicit shipping practices, country-specific due diligence, and Crown Dependency and Overseas Territory implementation. Sits alongside, rather than replaces, OFSI's separate oil price cap guidance.

B. Free and public vessel, ownership, and safety registries

Equasis — European Maritime Safety Agency (EMSA), with the IMO and over fifty other contributing bodies
https://www.equasis.org
A free ship database, registration required, covering more than 85,000 vessels above 100 gross tons. Pulls together registered and managing owner, flag history, classification society, insurer of record, and port state control inspection history in one place. The single best free starting point for a basic vessel and ownership check, though it displays what contributors submit rather than independently verifying it.

IMO GISIS (Global Integrated Shipping Information System) — International Maritime Organization
https://gisis.imo.org
The IMO's own public data hub, with free registration, covering ship and company particulars, casualty and incident reports, and treaty status across roughly two dozen modules. Authoritative for IMO numbers and formal regulatory status, though not built for compliance screening as such.

THETIS / Paris MOU port state control database — EMSA and the Paris Memorandum of Understanding on Port State Control
https://www.emsa.europa.eu/thetis.html
Records port state control inspections, detentions, and ship risk profiles across the Paris MOU region (most of Europe plus Canada). Useful for confirming detention history and flag-state performance ratings, but limited to that region's inspections rather than global coverage.

IACS Vessels in Class — International Association of Classification Societies
https://iacs.org.uk/membership/vessels-in-class/
A free lookup confirming whether a vessel's classification society is a current IACS member and the status of its survey. Narrow but reliable for exactly the question it answers.

International Group of P&I Clubs — the twelve mutual P&I clubs operating under the International Group Agreement
https://www.igpandi.org
Confirms which member club, if any, provides liability cover for a given owner. Since IG clubs collectively cover most ocean-going tonnage, absence of IG cover is itself a meaningful data point, though it doesn't by itself confirm what alternative cover (if any) exists.

C. Commercial integrated maritime risk and compliance platforms

Windward — Windward Ltd.
https://windward.ai
A behavioral-AI maritime intelligence platform built specifically around detecting deceptive shipping practices: AIS and GNSS manipulation, STS patterns, ownership networks, and sanctions exposure, with sanctions-list data from LSEG's World-Check integrated directly in. Positions itself on predictive detection, flagging high-risk vessels before formal designation, which is a genuinely useful capability if the underlying models hold up, though the specific accuracy figures it publishes are self-reported.

PurpleTRAC — Pole Star Global
https://www.polestarglobal.com/purpletrac/
A long-established (since the mid-2010s) sanctions screening and vessel monitoring platform, used by financial institutions and shipping companies alike, with a bill-of-lading and cargo-description screening add-on (DUG Screening) that most competitors don't offer in the same form. Draws sanctions data from Dow Jones Risk & Compliance under a data alliance.

Seasearcher — Lloyd's List Intelligence (Maritime Insights & Intelligence Limited)
https://www.lloydslistintelligence.com
Pairs machine-driven analytics with a network of human maritime analysts and Lloyd's Agents on the ground in major ports, which is a genuine differentiator from the more purely automated platforms. Its Risk & Compliance and Advanced Risk & Compliance tiers cover sanctions screening, AIS-gap and STS investigation, and up to seven levels of ownership.

Sea-web / Maritime Intelligence Risk Suite — S&P Global Market Intelligence (Maritime & Trade division)
https://www.spglobal.com/market-intelligence/en/solutions/sea-web-maritime-reference
The industry's largest maritime reference database by raw scale, over 220,000 ships and 600 data fields, built on S&P's position as the official issuing body for IMO ship and company numbers. Strongest as a reference and ownership-history tool; sanctions-specific risk overlays are a more recent addition (the Maritime Intelligence Risk Suite) layered on top of the core reference data.

D. Commodity flow, cargo, and freight intelligence

Kpler (including MarineTraffic and FleetMon) — Kpler
https://www.kpler.com
Kpler has absorbed both MarineTraffic and FleetMon into its ship-tracking product, giving it one of the broadest AIS networks in the industry alongside its original strength in cargo and commodity flow tracking. Publishes its own shadow-fleet risk-tree methodology publicly, which is a useful transparency practice most competitors don't match, and is frequently the data source cited in press coverage of specific shadow-fleet incidents.

Vortexa — Vortexa Ltd.
https://www.vortexa.com
Cargo- and grade-level tracking for crude, refined products, and LNG, going back to 2016, with a specific focus on identifying sanctioned or opaque cargo through multi-leg STS chains and floating storage. Vortexa estimates roughly fifteen percent of global seaborne crude is sanctioned or otherwise opaque by its own methodology; treat that figure, like all vendor-published market-share estimates, as an informed estimate rather than an audited count. Now integrated into Lloyd's List Intelligence's Seasearcher Cargo Risk module as a data source, alongside its own standalone platform.

E. Beneficial ownership and entity-resolution

Sayari — Sayari Labs
https://sayari.com
Purpose-built for tracing beneficial ownership through multiple layers of corporate structure, using primary-source registry filings across 250-plus jurisdictions rather than self-reported data, with explicit 50% Rule calculation. Not maritime-specific, it's a general corporate and trade-network due diligence platform, which makes it a natural complement to the maritime-focused platforms above rather than a replacement for them. Its main limitation is structural rather than technical: it can only trace what underlying registries actually publish, and some of the jurisdictions favored by shadow-fleet owners publish very little.

F. Sanctions-list and watchlist screening

OFAC Sanctions List Search — U.S. Department of the Treasury
https://sanctionssearch.ofac.treas.gov
The free, official tool for checking a name against the SDN List and the Non-SDN Consolidated List, using fuzzy name-matching. The primary source for U.S. sanctions status and the first stop for any American company, though it's a manual lookup tool rather than a batch-screening or monitoring system.

EU Sanctions Map — European Commission
https://www.sanctionsmap.eu
A free, visual reference tool covering both EU-autonomous and EU-implemented UN sanctions by country and theme. Useful for understanding the shape of an EU sanctions regime at a glance; not built for systematic screening integration, since it lacks the fuzzy matching a compliance system needs for that.

OpenSanctions — OpenSanctions Datenbanken GmbH
https://www.opensanctions.org
An open database aggregating several hundred sanctions, PEP, and other watchlist sources, free for non-commercial use with a paid API and data license for commercial use. A genuinely useful independent alternative or supplement to the large commercial vendors, and unusually transparent about its own matching methodology, though commercial deployment still carries a licensing cost like the vendors it's positioned against.

World-Check — LSEG (London Stock Exchange Group)
https://www.lseg.com/en/risk-intelligence/financial-crime-risk-management/sanctions-screening
One of the two dominant curated sanctions and PEP screening datasets in financial-crime compliance broadly, covering over 300 sanctions programs with a large dedicated research staff. Appears as an integrated data source inside Windward and other maritime platforms rather than only as a standalone product in this context.

Dow Jones Risk & Compliance — Dow Jones
https://www.dowjones.com/professional/risk/
The other of the two dominant curated screening datasets, and notably the data partner behind Pole Star's PurpleTRAC. Covers sanctions, PEP, and adverse media, with specific content built around the OFAC and EU 50% Rule for indirect ownership exposure.

G. Independent vessel geolocation and remote sensing

Spire Maritime — Spire Global, Inc.
https://spire.com
Operates its own satellite AIS receiver network plus RF-based dark-vessel detection, giving it visibility that doesn't depend on any single terrestrial AIS provider. Partners commercially with BlackSky and ICEYE to combine RF detection with imagery confirmation.

HawkEye 360 — HawkEye 360, Inc.
https://www.he360.com
A constellation of small satellites flown in clusters of three, geolocating radio frequency emissions (marine radar, VHF radios, satellite communications) independent of AIS entirely. This is the layer that can find a vessel that has gone fully dark, as long as it's still emitting some other detectable signal, and has documented real cases (including an AIS-dark vessel traced to a Syrian port) publicly.

ICEYE — ICEYE
https://www.iceye.com
Synthetic aperture radar (SAR) satellite imagery, which images through cloud cover and darkness, unlike optical satellites. Particularly effective for catching ship-to-ship transfers in progress, since two vessels alongside each other at sea show up clearly in a SAR image regardless of weather or time of day. Capella Space is a comparable SAR provider frequently used alongside or instead of ICEYE in this same role.

BlackSky — BlackSky Technology Inc.
https://www.blacksky.com
High-revisit optical satellite imagery with tasking latency the company advertises as under two hours, used to visually confirm a vessel's identity or condition once RF or SAR data has already narrowed down where to look. Best understood as the confirmation layer that follows RF or SAR detection, not a first-detection tool on its own.

H. Open-source and NGO investigative trackers

Russian Shadow Fleet Tracker — KSE Institute (Kyiv School of Economics)
https://kse.ua/sanctions-hub-of-excellence/
A free monthly analytical product tracking Russian shadow-fleet oil shipments: cargo destinations, vessel ownership patterns, fleet composition changes, and insurance arrangements. Independent, methodologically transparent, and specifically useful for understanding current scale and trend rather than screening an individual counterparty transactionally.

UANI Tanker Tracker — United Against Nuclear Iran (built on its MINERVA vessel-behavior system)
https://www.unitedagainstnucleariran.com/tanker-tracker
An advocacy organization's ongoing public tracking of vessels suspected of moving Iranian oil, combining AIS analysis with satellite imagery and, at times, human intelligence. Widely cited by journalists and cross-referenced by other maritime data vendors; useful for spot-checking a specific vessel name against a well-documented public record, though it's an advocacy product with a stated policy position, not a neutral compliance vendor.

Appendix: Use Cases for Sections C, D, G, and H

The synopses above describe what each tool does. What follows is how that plays out in practice, for the tools in sections C, D, G, and H specifically, since those are the ones most often described only by their feature list. Each numbered item is an illustrative scenario grounded in the tool's documented capabilities, not a reported case, except where noted otherwise.

C. Commercial integrated maritime risk and compliance platforms

Windward

1. Your chartering desk is about to fix a tanker for a cargo lift and needs to clear the vessel before signing. A plain sanctions-list check would come back clean, since the vessel isn't formally designated yet, but Windward pulls up its behavioral score anyway: recent AIS gaps in a known STS corridor, an ownership change six weeks ago, a jump in risk rating. It returns a go, escalate, or no-go recommendation with the evidence attached, in minutes, so it fits inside the negotiation window rather than delaying it. This is a real-time, transaction-level check.
2. Your trade finance desk has already financed a dozen cargo shipments, and the vessels involved were clean at onboarding. Windward re-screens the existing book continuously and pushes an alert if any of those vessels' risk scores cross a threshold later, catching drift, a reflag, a new STS pattern, that a one-time check at onboarding would never see. This is ongoing portfolio monitoring, not a point-in-time lookup.

PurpleTRAC (Pole Star Global)

1. A cargo arrives with a bill of lading claiming a certain origin and goods description. Before your team accepts it, PurpleTRAC's document-screening module (DUG Screening) checks that description and discharge country against 26 restricted-goods and sanctioned-region lists and returns an OK, Warning, or Critical flag in near-real time, catching the specific falsified-certificate pattern OFAC has called out by name.
2. Your compliance officer needs to screen the whole existing vessel and counterparty list weekly and produce something a regulator would accept as evidence of due diligence. PurpleTRAC runs that as an automated batch job and stores the reports for retrieval, a periodic, scheduled process rather than a one-off check, where the output is the audit trail itself, not just the answer.

Seasearcher (Lloyd's List Intelligence)

1. A vessel your company chartered went dark for four days, and a news report afterward suggests something happened during that window. This is a post-mortem: your team needs to reconstruct the voyage to decide whether to escalate internally, notify a regulator, or exit the relationship. Seasearcher's analysts and Lloyd's Agents rebuild the voyage from multiple independent sources and produce a timeline flagging any STS activity or dark port calls, typically over hours to a few days, since it involves human review, not an instant automated answer.
2. A new ship owner approaches your company as a potential long-term counterparty, and you need a first-pass due diligence pull before the relationship starts. Seasearcher returns ownership up to

seven levels deep, sanctions status, and casualty and detention history in one same-day report.

Sea-web / Maritime Intelligence Risk Suite (S&P Global)

1. An insurer is pricing a hull policy and needs accurate technical specifications and ownership history to confirm the vessel hasn't passed through a sanctioned owner's hands at some point. Sea-web is the reference-grade source for that: over 600 data fields per vessel, with historical name, owner, and flag changes going back through the vessel's life. This is a static, on-demand reference lookup rather than a monitoring function, essentially instant retrieval used as one input into a pricing decision that itself takes longer.

D. Commodity flow, cargo, and freight intelligence

Kpler (including MarineTraffic and FleetMon)

1. A trading desk is offered a cargo that changed hands via an open-ocean STS transfer and has only the seller's word for what it actually is. Kpler correlates both vessels' AIS tracks, models the transfer, and estimates the cargo grade and volume that moved, cross-checked against its own shadow-fleet list. This is a same-day, pre-purchase check, not instantaneous, since reconstructing a specific past event takes some processing.
2. Your risk function wants to know whether shadow-fleet activity is rising in a corridor the company operates in, as a signal to tighten internal thresholds before a specific transaction forces the question. Kpler publishes aggregate flow and dark-fleet trend data monthly, a strategic, periodic input into policy review rather than a transaction-level tool.

Vortexa

1. You're buying a cargo of Russian-origin refined product, and the seller attests the price was under the G7 cap. Price-cap compliance runs on attestation, not physical verification, so you need a same-day sanity check: Vortexa's grade-level market pricing and freight data let you confirm the attested price is plausible against what the market was actually doing that week.
2. A vessel presented to your chartering team looks slightly off, unusually capable specs for its claimed age. Vortexa's cargo and fleet-movement history can surface the kind of inconsistency that points to a "zombie tanker," a scrapped hull's identity reused to move cargo under a clean-looking name, before your team commits to the charter.

G. Independent vessel geolocation and remote sensing

Spire Maritime

1. Vessels you charter transit open ocean where terrestrial AIS coverage is thin, and a legitimate coverage gap looks identical to deliberate manipulation from the outside. Spire's satellite AIS network fills that gap with near-real-time position data, some latency versus terrestrial AIS, but still operationally current, so your team isn't flagging a routine dead zone as evasion.
2. A chartered vessel's AIS went fully silent for four days in a high-risk corridor, and you need an independent read on where it actually was. Spire's RF-monitoring satellites can pick up other emissions from the vessel, radar, VHF, during that window and estimate its position. This is retrospective, typically turned around over a few days once tasked, not instant.

HawkEye 360

1. An AIS gap lines up with just enough time for a vessel to have reached a sanctioned port, and your compliance team needs to know whether it actually went there before deciding how to respond. HawkEye 360 geolocates the vessel's other radio emissions during that specific gap window to answer that question. This is a tasked, retrospective investigation, resolved over days as its satellites pass over the area, and it's exactly this capability that let it publicly trace an AIS-dark cargo vessel to a Syrian port in a documented 2021 case.
2. Before investing in or servicing a port in a region known for shadow-fleet activity, you want an independent read on how much dark-vessel traffic actually passes through, not just what's officially reported. A regional RF sweep over some days to weeks establishes that baseline as part of the due diligence, rather than confirming any one vessel.

ICEYE

1. Two vessels' last known positions before going dark suggest they may have met at sea. If that inference matters, say, to a decision about exiting a counterparty relationship or filing a report, you want visual confirmation, not just inference. ICEYE tasks a synthetic aperture radar satellite over the suspected location; because SAR sees through cloud and darkness, it can catch two vessels alongside each other regardless of weather. This is a tasked, investigative pull, typically same-day to a few days depending on the satellite's revisit schedule.
2. You suspect a vessel is repeatedly loitering at a known STS anchorage rather than making a one-off legitimate stop. Repeated ICEYE passes over the same location, spread across days to weeks, build the time series that turns a single suspicious sighting into an established pattern.

BlackSky

1. RF or SAR has narrowed a dark vessel down to a location but can't put a name to it. BlackSky tasks a high-resolution optical satellite for a close look, which the company markets as arriving within roughly 90 minutes of a request, the fastest of the imagery layers, though still dependent on daylight and clear skies since it's optical rather than radar. This is the confirmation step that typically follows an RF or SAR detection, not a first-detection tool on its own.
2. An independent read on vessel traffic and congestion at a specific high-risk port over time is useful since official port-call records for some ports are incomplete or simply not published. Repeated imaging over days to weeks builds that picture.

H. Open-source and NGO investigative trackers

Russian Shadow Fleet Tracker (KSE Institute)

1. Your compliance team is deciding how aggressive to set internal shadow-fleet criteria, an age cutoff, how much scrutiny a non-IG insurer gets, and wants an independent benchmark rather than relying entirely on a vendor's undisclosed methodology. KSE's monthly, methodologically transparent tracker gives current data on typical shadow-fleet vessel age, ownership jurisdictions, and insurance patterns to calibrate against. This is periodic and strategic, used to set or revisit policy, not to clear an individual transaction.
2. A vessel name comes up in a proposed charter, and before paying for a full commercial screening pull, someone runs the name against KSE's public reporting to see if it's already been flagged. This is on-demand, free, and fast, a supplement to paid screening rather than a replacement for it.

UANI Tanker Tracker

1. A vessel in a proposed transaction has some connection to routes UANI covers, and you want an independent cross-reference specifically on the Iran side, where UANI's tracking is particularly well regarded. Its public reporting, refreshed roughly monthly and built on AIS analysis, satellite imagery, and its MINERVA behavioral system, gives a same-day reference check against a regularly updated public record.
2. Leadership wants a periodic, plain-English update on how Iranian oil sanctions evasion is trending, to inform a strategic decision about the company's exposure in the region, not the compliance-officer-level detail a vendor platform provides. UANI's monthly tracker functions as that briefing input.

A closing note on how to use this: no single item above, free or paid, is sufficient by itself. The tools that work best in practice combine independently sourced position data (to catch AIS manipulation), ownership-tracing (to catch shell structures), and list screening (to catch what's already been designated), because each catches a different piece of the same underlying evasion pattern. Building that combination, and deciding how much of it to buy versus assemble from free sources, is a resourcing decision that depends on the company's actual exposure, not a one-size answer.