Price Cap Coalition

Oil Price Cap (OPC) Compliance and Enforcement Alert

1 February 2024

OVERVIEW

The oil price cap (OPC), introduced by the "Price Cap Coalition" (or "G7+ Coalition", comprising the G7, the European Union, and Australia) in December 2022, has two key objectives: 1) constraining Russian revenues that could otherwise be used to fund Russia's war of aggression against Ukraine; while 2) maintaining global oil flows and protecting energy security.

The OPC has been designed with industry in mind and the Price Cap Coalition expects that legitimate industry stakeholders involved in the trade of Russian oil and oil products strengthen their compliance with the OPC. However, we must remain vigilant to cases where inadvertent circumvention or misinterpretation of the OPC occurs, or where certain actors evade the measure while operating within an otherwise compliant chain of industry stakeholders. Illicit activity could occur across multiple entities and sectors involved in the trade of Russian oil and oil products. Poor and insufficient compliance processes by the entities involved could lead to breaches of the OPC.

The Price Cap Coalition takes a proactive compliance and enforcement approach. This includes supporting governments and industry stakeholders to improve their compliance with the OPC, identifying suspected evasion and breaches of the OPC, and taking robust enforcement action where necessary.

This alert includes:

- An overview of key OPC evasion methods and recommendations for identifying such methods and mitigating their risks and negative impacts.
- Information on how to report OPC suspected breaches across the Price Cap Coalition.

The OPC evasion methods covered in this alert are related to:

- Falsified documentation and attestations.
- Opaque shipping and ancillary costs.
- Third country supply chain intermediaries and complex and irregular corporate structures.
- Flagging.
- The "shadow" fleet.
- Voyage irregularities.

This alert builds on the "Coalition Statement on Price Cap Rule Updates" (20 December 2023) and previous guidance issued by the Price Cap Coalition and its members such as the: Price Cap Coalition Maritime Safety Advisory (12 October 2023); Office of Financial Sanctions Implementation (OFSI) Maritime Guidance (December 2020) and UK Maritime Services Ban and Oil Price Cap Industry Guidance; Office of Foreign Assets Control (OFAC) Alert on Possible Evasion of the Russian Oil Price Cap (April 2023) and Guidance on Implementation of the Price Cap Policy; and the European Commission's Oil Price Cap Guidance.

Industry stakeholders involved in the trade of Russian oil and oil products should consider this alert in full. By adopting the recommendations included in this alert and previous guidance documents, governments and industry stakeholders can improve their compliance with the OPC and reduce their exposure to possible risks associated with circumvention and evasion of the measure.

Evasion methods outlined in this alert could be seen separately or be interlinked and part of a broader set of illicit activity. Risk profiles are dynamic and may change over time. Monitoring should take into account legitimate reasons for apparent evasion red flags (e.g., to manage security risks to vessels in high-risk areas).

Industry stakeholders should pay particular attention to evasion types and recommendations related to their specific areas of work, and of other entities they engage with in the trade of Russian oil and oil products.

Industry stakeholders are encouraged to share this alert within their organisations and with entities they interact with throughout the supply chain. Relevant industry associations are also encouraged to share this alert with their members, which they can complement with their own detailed advisories to include sector specific recommendations and case studies.

This alert is not legal advice and governments and industry stakeholders using it are encouraged to seek their own independent legal advice as necessary.

OPC EVASION METHODS AND RECOMMENDATIONS

OPC evasion methods: what do I need to look for?

Falsified documentation and attestations

Complete and accurate OPC attestations and transaction and shipping documentation are crucial to ensure compliance with the OPC. Falsified documentation can be used to disguise the true price paid for Russian oil and oil products and obscure the origin of a vessel, its goods, destination, and even the legitimacy of the vessel itself. This could lead to Coalition services inadvertently being used to support non-price cap compliant transactions.

Opaque shipping and ancillary costs

Manipulation of shipping and ancillary costs (including shipping, freight, customs, and insurance costs), the bundling of such costs, and failure to itemise these costs could be used to obfuscate Russian oil and oil products being purchased above the price cap. These costs should be at commercially reasonable rates, in line with industry standards, including any geopolitical risk premiums. The billing of commercially unreasonable or opaque shipping and ancillary costs should be viewed as a sign of potential OPC evasion.

The Coalition statement of 20 December 2023 announced revisions to the price cap compliance regime including: 1) that relevant Coalition service providers will be required to receive attestations from their counterparties each time they lift or load Russian oil or oil products; and 2) changes that will require supply chain participants with access to itemised ancillary costs (e.g., insurance and freight) to share these upon request with entities further down the supply chain. These changes will support the implementation of the OPC and disrupt circumvention by reducing opportunities for bad actors to use opaque shipping costs to disguise oil purchased above the cap.

Third country supply chain intermediaries and complex and irregular corporate structures

Entities attempting to evade the OPC are increasingly looking to third country supply chain intermediaries and the use of complex and irregular corporate structures to trade Russian oil and oil products. Many of these enablers and facilitators are legitimate entities but some are deliberately trying to evade the OPC while using Coalition services. This includes the use of shell companies, multiple levels of ownership and management to disguise the ultimate beneficial owner of Russian oil and oil products, and frequent changes in the ownership or management of companies and vessels involved. OPC evasion red flags would be seen, for example, if a recently formed company, with no obvious links to or history with Russian oil trade and with opaque funding sources, in a short period of time bought several vessels to trade Russian oil and oil products, as such companies may be more likely to engage in deceptive practices.

Recommendations: what do I need to do?

Appropriate and enhanced due diligence

Industry stakeholders should undertake appropriate due diligence of customers and counterparties across the supply chain that they engage with in the trade of Russian oil and oil products. This is especially important where Coalition services are being used or sought and there are OPC evasion red flags. In this context, where business intelligence, information, or market assessments indicate that Russian oil or oil product prices exceed the price cap, industry stakeholders should not provide the service and should notify the relevant authorities.

Industry stakeholders' due diligence should be calibrated according to the specificities of their business and the related risk exposure. They should institutionalise effective sanctions compliance programmes and monitoring for OPC evasion red flags. They should identify and manage risks including through appropriate due diligence and Know Your Customer (KYC) and Know Your Customer's Customer (KYCC) procedures, the latter of which can be used to identify ultimate beneficial ownership, including any links to Russian entities.

Industry stakeholders should risk assess documents that appear incomplete, inconsistent, or contradictory to previously shared or publicly available information, as this may suggest illicit activity. They are encouraged to retain documents showing that Russian oil or oil products were purchased at or below the relevant price cap (e.g., invoices, contracts, and receipts/proof of payment). These documents should be shared, as necessary, with other service providers throughout the supply chain and at the request of Coalition authorities. Alternative documentation and information sources should also be used to corroborate the information held as necessary (e.g., to check that ship registration documents match with insurance documents).

Enhanced due diligence may be appropriate for ships that have undergone numerous administrative changes (e.g., re-flagging or being sold), when they involve complex and irregular corporate structures, and when dealing with intermediary companies (e.g., management companies, traders, and brokerages) that conceal their beneficial ownership or otherwise engage in unusually opaque practices.

Industry stakeholders' due diligence assessments should be used to build risk profiles of particular vessels and companies that they engage with in the trade of Russian oil and oil products. This due diligence may help inform an internal "whitelist" of entities considered ordinarily compliant with the OPC, and with whom routinely conducting business may offer reduced risk exposure. OPC evasion methods, prevalence, and risk profiles are dynamic and may change over time, and therefore entities on any such whitelist should be regularly reviewed.

OPC evasion methods: what do I need to look for?

Flagging

Certain flagging and reflagging activities may indicate that a vessel is attempting to obfuscate its true ownership and/or affiliation with Russia and should be considered high-risk and warrant enhanced compliance and KYC checks.

These activities may include where a vessel:

- Uses a false flag to mask illicit trade in which the vessel continues to use a country's flag after it has been removed from a registry (i.e., "deregistered") or claims a country's flag without proper authorisation.
- Has changed flag on multiple occasions in a short period of time ("flag hopping") to avoid detection.
- Previously registered under the Russian flag has changed to a different flag registry since the OPC was implemented.
- Is flagged with registries known to employ insufficient KYC and compliance checks upon registering vessels.

"Shadow" fleet

The "shadow" fleet (also referred to as the "ghost," "dark," or "parallel" fleet) generally refers to older vessels that are anonymously owned and/or have opaque corporate structures that are solely deployed in the trade of sanctioned oil or oil products and engage in various deceptive shipping practices.

There is ample evidence that Russia has utilised these vessels to transport its oil and oil products. Whilst these vessels may be compliant with relevant laws, or not covered by them, these vessels have given Russia an outlet for its oil exports and a means to circumvent sanctions in a more unfettered way, with arguably limited exposure and without clear attribution.

The shadow trade also involves ships that may rely on unknown, untested, sporadic, or fraudulent insurance. Without legitimate, continuous insurance coverage, these ships may be unable to pay the costs of accidents in which they are involved, including oil spills, which entail tremendous environmental damage, significant safety risks, and extensive costs.

Some ships have also shifted away from industry standard classification societies, which play a key role in assessing and ensuring the seaworthiness of vessels, adding to environmental and safety concerns.

Recommendations: what do I need to do?

Flagging

Flagging registries should inform registrants and owners of vessels through marine notices that sanctionable or illicit conduct would be cause for immediate removal of registration. They should also share relevant information on OPC evasion with other flagging registries and competent authorities, as appropriate. This includes the names and IMO numbers of vessels that have been denied registration or deregistered due to apparent non-compliance.

Industry stakeholders may benefit from consulting available industry resources such as the International Chamber of Shipping's (ICS) Flag State Performance Table (link), where "potentially negative performance" indicators may be useful, as part of a broader set of information, to help inform sanctions risk assessments.

"Shadow" fleet

Industry stakeholders should undertake enhanced due diligence of vessels which fit the shadow fleet description and are used to transport Russian oil and oil products.

Some Coalition Members (including the European Union, link) have introduced measures to more closely monitor the sale of tankers to third countries and prevent them from being used to transport oil priced above the cap. Industry stakeholders are encouraged to report to relevant competent authorities tanker sales they observe which display evidence to indicate that they could be used as part of the shadow fleet.

Industry stakeholders should consult the International Maritime Organization (IMO) resolution "A.1192(33) Urging Member States and all relevant stakeholders to promote actions to prevent illegal operations in the maritime sector by the 'dark fleet' or 'shadow fleet'."

To mitigate against increased environmental and safety risks associated with the shadow fleet, industry stakeholders are encouraged to require that such vessels have continuous and appropriate maritime insurance coverage for the entirety of their voyages; and that they be insured by legitimate insurance providers with sufficient coverage for International Convention on Civil Liability for Oil Pollution Damage (CLC) liabilities. If an industry stakeholder is engaging with a ship that is not insured by such a legitimate insurance provider, they should conduct sufficient due diligence to ensure that the insurer can cover all relevant risks. This could include, as feasible, a review of an insurer's financial soundness, track record, regulatory record, and ownership structure.

Industry stakeholders are encouraged to ensure counterparties receive classification from the International Association of Classification Societies (IACS) member classification societies to ensure vessels are fit for the service intended.

OPC evasion methods: what do I need to look for?

Voyage irregularities

Voyage details should normally be known and traceable, from the port of loading to the final destination. While there may be legitimate reasons for possible changes to this, illicit actors may attempt to disguise the ultimate destination, origin of cargo, or recipients by using indirect routing, unscheduled detours, or transit or transshipment of cargo through third countries.

There are legitimate reasons for Automatic Identification System (AIS) to be turned off or "go dark" (e.g., passage through waters at high-risk of piracy or due to other security considerations). In such situations, it is advisable for ships to turn off their AIS to evade threats, and thus should not be considered a red flag for illicit activity. However, AIS manipulation and spoofing could be used to evade the OPC (e.g., to disguise which ports particular vessels have visited and their whereabouts for the purpose of evading detection when conducting illicit trade). Repeated, prolonged, and unexplained gaps in AIS, particularly in sensitive locations as well as unusual transmissions, should be cause for further investigation.

Ship-to-ship (STS) transfers often have legitimate uses (e.g., providing flexibility for cargo owners and for taking advantage of economies of scale). However, STS transfers can also be used to conceal the origin, nature, and destination of cargo and therefore be used to evade the OPC. This includes through ignoring pre-notification and reporting obligations under international law, being done at night and in areas known for illicit behaviour, and in conjunction with other evasion practices such as AIS manipulation or "spoofing." STS transfers of crude oil or oil products outside of safe and sheltered waters also entail heightened environmental and safety risks.

Recommendations: what do I need to do?

Voyage irregularities

Relevant industry stakeholders should be able to explain voyage and shipment details. Industry stakeholders should conduct enhanced monitoring of vessels and regions which display evidence of voyage irregularities, AIS manipulation and spoofing, and illicit STS transfers. This should take into account legitimate reasons for apparent voyage irregularities (e.g., to manage security risks to vessels in high-risk areas). There are a number of maritime and sanctions intelligence and assessment tools to support this.

Industry stakeholders are encouraged to scrutinise routes and destinations that deviate from normal business practices for unknown reasons, including routine transit and transshipment. They should also stay aware of locations known for STS transfers associated with deceptive or evasive activity, particularly in combination with AIS manipulation and/or previous voyage history.

Relevant industry stakeholders are encouraged to investigate signs and reports of AIS manipulation before entering into new contracts or when engaging in ongoing business. They should also consider incorporating contractual language, and explicitly notify clients, that AIS disablement or manipulation inconsistent with the International Convention for the Safety of Life at Sea ("SOLAS") is possible grounds for investigation of the ship's activities and could result in cancellation of service provision if illicit or sanctioned activity is identified.

If a vessel cannot account for its AIS history consistent with SOLAS, port authorities may wish to consider investigating the underlying activity (e.g., check records and/or the logbook). If determined to be sanctioned or illicit, the port authorities may wish to consider prohibiting that vessel from entering their ports or taking other appropriate actions.

No single vessel behaviour should be viewed in isolation. A legitimate operation between a vessel and a partner vessel may still present an exposure to sanctions if the partner vessel has previously engaged in an STS operation with a vessel carrying Russian oil or oil products above the price cap or other sanctioned cargo.

HOW TO REPORT OPC SUSPECTED BREACHES ACROSS THE PRICE CAP COALITION

Coalition member	OPC compliance and enforcement approach	How to report OPC suspected breaches
Australia	The Australian Sanctions Office (ASO) within the Department of Foreign Affairs and Trade works with co-regulators and enforcement partners, including the Australian Border Force, the Australian Federal Police, Department of Defence, and others to implement and enforce sanctions, including with the OPC. Contravening sanctions is a serious offence that can attract criminal and/or civil penalties.	Potential contraventions of the OPC should be reported by emailing: sanctions@dfat.gov.au.
Canada	Global Affairs Canada (GAC) works with enforcement agencies, including the Canadian Border Services Agency and the Royal Canadian Mounted Police (RCMP), to implement and enforce sanctions, including the OPC. Contravening sanctions is a criminal offence, punishable by fines and/or imprisonment.	Potential violations of the OPC should be reported to the RCMP by emailing: Federal_Policing_Intake_Unit@rcmp-grc.gc.ca.
European Commission	EU Member States are responsible for the implementation and enforcement of EU sanctions, as well as identifying breaches and imposing penalties for violation of the OPC. The European Commission ensures uniform implementation and monitors enforcement of EU sanctions by EU Member States and supports them in this task.	Suspected breaches can be reported via the Whistleblower tool: https://eusanctions.integrityline.com or by email: relex-sanctions@ec.europa.eu.
France	The French Treasury works with enforcement agencies, in particular the Customs Agency which is competent to lead the investigations. Contravening sanctions is a criminal offence, punishable by fines and/or imprisonment.	Suspected OPC breaches should be reported to the French Treasury by emailing: sanctions-russie@dgtresor.gouv.fr
Germany	While the coordination of Germany's sanctions policy lies with the Federal Foreign Office, sanctions enforcement and prosecution of suspected violations involve various agencies within the scope of their respective competencies, such as customs and maritime and law enforcement authorities.	Pursuant to article 6b para. 1 a) of Council Regulation (EU) 833/2014 (containing OPC related provisions) any "information which would facilitate the implementation of the Regulation" (including information on (attempted) breaches) has to be reported to the competent authorities of the Member States. Competent authorities in Germany are the following: • For funds, financing, and financial assistance (including insurance): Deutsche Bundesbank (sz.finanzsanktionen@bundesbank.de). • Goods and goods-related services: Bundesamt für Wirtschaft und Ausfuhrkontrolle (ru-embargo@bafa.bund.de). • Enforcement in German waters/ maritime transport related aspects: Joint Emergency Reporting and Assessment Centre Sea (JERACS) (contact). • Others: Auswärtiges Amt – Sanctions Policy Task Force (contact). Potential breaches of EU-restrictive measures should be reported to the regular investigative authorities who are exclusively competent for conducting respective (criminal) investigations.

Italy	Involvement of various agencies within the scope of their respective competencies: the Border and Financial police (Guardia di Finanza), the Customs Agency, and the Coast Guard.	Each agency has its own reporting system, please refer to their respective websites: Guardia di Finanza; the Customs Agency; and the Coast Guard.
Japan	Foreign Transactions Control Office of the Ministry of Finance (MOF) works for the implementation and enforcement of sanctions, including the OPC, with the Financial Services Agency, the Ministry of Foreign Affairs, the Customs and Tariff Bureau of the MOF, the Ministry of Economy, Trade and Industry, and the Ministry of Land, Infrastructure, Transport and Tourism. Contravening sanctions is a criminal offence, punishable by fines and imprisonment.	Potential violations of the OPC should be reported to the Foreign Transactions Control Office of the MOF: +81-3-3581-4246.
UK	The UK undertakes strong and proactive enforcement of the OPC. The Office of Financial Sanctions Implementation (OFSI) is responsible for civil enforcement, and HM Revenue and Customs (HMRC) and the National Crime Agency (NCA) jointly consider cases which may be appropriate for criminal prosecution. OFSI's OPC guidance can be found here.	Suspected breaches should be detailed in an OPC breach reporting form found here, with the completed form and supporting documentation sent to OFSI who will investigate as necessary.
United States	The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals, and has broad authority to take action against actors that evade the price cap. OFAC's OPC guidance can be found here.	Information or questions about sanctioned parties or potentially sanctionable or prohibited activity may be submitted to this email address: OFAC_Feedback@treasury.gov.