Financial Intelligence Unit - Jersey

INTEL INSIGHT

Intelligence Insight

SUBJECT:

Russian Oil Price Cap Evasion

DATE:
08 May 2025

CATEGORY LEVEL:

GREEN > Information / Awareness
ALERT

This Intelligence Insight report is issued by the Financial Intelligence Unit - Jersey (FIUJ). The FIUJ serves as Jersey's national intelligence agency and competent authority responsible for the receipt, analysis and dissemination of intelligence developed from the submission of Suspicious Activity Reports (SARs) and other reporting and analysis capabilities, aligned with Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) reporting obligations.

This GREEN Alert Report is produced for the purposes of sharing information, training or general awareness. It should be used widely by distributed stakeholders, and it is recommended you use this Alert to complement existing knowledge and support ongoing improvements to business protocols.

INTEL INSIGHT

Financial Intelligence Unit - Jersey

DATE: 08 May 2025

DISTRIBUTION: Public / Training

CATEGORY LEVEL: GREEN – Information / Awareness

Russian Oil Price Cap Evasion

The "So What" for Jersey

- If Jersey institutions are implicated in Oil Price Cap Evasion, the jurisdiction would likely suffer **reputational damage** and face censure from the UK, as well as potentially from the EU and the US. This could ultimately undermine Jersey's credibility as a professional and reliable IFC, deterring legitimate enterprises and consequently harming the island's economy.
- Subject to **FATF standards**, Jersey is assessed on its sanctions law and enforcement measures; a failure in this regard could result in subsequent action by MONEYVAL.
- Institutions found to be connected to Oil Price Cap Evasion, thus consequently aiding Russia's war effort, have faced secondary US sanctions or EU **penalties**. Such facilitation can lead to punitive actions, including financial repercussions.
- Jersey-administered shipping entities are at risk of intermediary **exploitation** in complex structures.
- Jersey's TCSP sector is open to the risk of exploitation. Bad actors may attempt to obscure the identity of **beneficial owners** and develop layers of corporate structure while concealing the true nature of the business and the origin of funds.
- Hostile states / threat actors may view Jersey as a gateway to the UK, seeking to exploit perceived weaknesses of an IFC.
- British accountants have been involved in oil price cap circumvention. Therefore, there is potential **vulnerability** regarding the accountancy sector.[1]
- Russia's Shadow Fleet continues to use third-party jurisdictions to host its tankers. These **high-risk geographies** may pose a threat to Jersey if there are jurisdictional business ties, such as overlaps between Jersey's key markets and Shadow Fleet activities.

INTELLIGENCE QUESTION:	• What is Russian Oil Price Cap Evasion and • What is Jersey's exposure?
INTELLIGENCE ASSUMPTION:	• As an IFC, Jersey may be exposed to intermediary exploitation in complex structures seeking to facilitate oil price evasion.
INTELLIGENCE GAPS OR IDENTIFIED RISKS:	• If oil price cap evasion is linked to Jersey, then there is a risk to jurisdictional reputation and incurring potential legal penalties. • Some proactive education, training and understanding of evasion methods and typologies could assist to mitigate threats posed.

[1] Financial Times, 'Russia's shadow fleet grows despite western crackdown' (Financial Times, October 2024)

Overview

1. In response to Russia's illegal invasion of Ukraine in February 2022, the UK, alongside G7 countries, Australia and the EU, implemented a price cap of USD 60.00 per barrel of oil. The purpose of this was to restrict the Russian economy's oil revenues, without causing a spike in global oil prices. The price cap was enacted in December 2022, restricting western companies from transporting, servicing or brokering Russian oil cargoes.[2]

2. Over two years after the oil price cap was introduced, Russia is estimated to have spent USD 10 billion in developing a 'Shadow Fleet', to circumvent sanctions and sell oil above the USD 60.00 threshold.[3] Before 2022, Russia's oil trade heavily relied on Western-owned and insured tankers; however, due to Western sanctions, Russia has had to develop its own oil trade fleet. This fleet consists of more than 630 tankers. The average age of a vessel in this fleet is 18 years, and the majority are uninsured.[4] Despite Western efforts, Russia is currently transporting nearly 70 percent of Russian oil via this shadow fleet, selling above the established threshold, ultimately aiding Russia's war effort.[5]

3. As the war persists, more attention is being drawn to the price cap, as the loose enforcement of the policy has marred its effectiveness. However, the British Government is now conducting thirty-seven investigations into UK-linked businesses that may have broken Russian oil sanctions, which signals a future commitment to this policy.[6] Furthermore, the European Union is preparing to add over 100 vessels belonging to Russia's Shadow Fleet to its next package of sanctions levied against Russia.[7] On 10 January 2025, the United States, through its Office of Foreign Assets Control, imposed a new round of sanctions aimed at countering ongoing price cap evasion. This expanded the list of sanctioned vessels, targeting an 'unprecedented number' of 183 tankers belonging to Russia's Shadow Fleet.[8]

FIU COMMENT

Russia's success in circumventing the oil price cap has likely supported its ability to contribute to military spending and thus finance its war in Ukraine. As the conflict endures, the British Government and Price Cap Coalition will likely seek to enforce firmer measures against evasion, as demonstrated by ongoing investigations and forthcoming European Union sanctions.

FIU COMMENT

Jersey offers a range of services to shipping entities, potentially exposing the island to risks associated with intermediary exploitation within complex structures. This vulnerability underscores the necessity for Jersey to adopt a proactive approach, ensuring continuous vigilance and awareness of emerging methods and typologies. These methods are developed and implemented on a state level. Therefore, the level of sophistication required to engage in price cap evasion goes beyond the familiar capabilities of criminal networks.

FIU COMMENT

Attention to red flag indicators is vital in discerning potential bad actors; industry should be aware of evasion methods relating to the oil price cap and the relevant risks. Enhanced measures are necessary when engaging with high-risk jurisdictions pertaining to price cap evasion enablement. There are known

[2] Eric Van Nostrand, Anna Morries, 'Phase Two of the Price Cap on Russian Oil: Two Years After Putin's Invasion' (U.S. Department of the Treasury, February 2024)
[3] Alan Rappeport, 'Russian Oil Flows Through Western Price Cap as Shadow Fleet Grows' (New York Times, October 2024)
[4] Jonathan Saul, 'Growing armada shipping sanctioned oil burns fuel in setback for clean-up efforts' (Reuters, May 2024)
[5] Anastasia Stognei, 'Russia's shadow fleet grows despite western crackdown' (Financial Times, October 2024)
[6] Jack Fenwick, 'UK-linked firms suspected of busting Russia sanctions' (BBC, October 2024)
[7] Brendan Cole 'Europe Prepares New Blow to Putin's Shadow Fleet' (BBC, May 2025)
[8] Marcus Hand 'US sanctions unprecedented number of shadow fleet ships' (Seatrade Maritime News January 2025)

and well-documented hotspots for Shadow Fleet activity, such as Gabon. Russia transferred at least 85 vessels from Liberia to Gabon last year, 40 of which operated routes directly from Russian ports to China, India and Turkey.[9]

Evasion Methods

4. Bad actors are increasingly utilising sophisticated and creative methods to avoid detection. Simple checks to establish whether a vessel or related entity is on the sanctions list are no longer sufficient to determine possible exposure.

False Flags / Flag Hopping

5. Vessels attempting to bypass sanctions, including the oil price cap, have been utilising flagging and reflagging methods, where a vessel attempts to disguise its true ownership / connection with Russia. Red flags include:

   - A vessel sails under another country's flag, particularly one not subject to the oil price cap rules. For example: Under flag of Gabon, tankers sail sanctioned Russian oil through Arctic Ice.
   - A vessel is flagged with registries known for insufficient KYC and compliance checks.
   - A vessel previously registered under the Russian flag has changed flag registry since the price cap was introduced.
   - A vessel has changed flags numerous times (flag hopping) in a short period of time.
   - A vessel claims a nation's flag without legitimate authorisation.

Complex Ownership / Management

6. The Russian shadow fleet makes use of grey-listed flag states and the subsequent benefits of anonymous ownership structures. These often include multiple intermediaries. An investigation from the Financial Times exposed British accounts and Dubai-based companies hidden through layers of corporate entities involved in circumventing the oil price cap. Red flags include:

   - Newly founded entities.
   - No identifiable beneficiary or ultimate beneficiary links.
   - Company hopping in a short period of time.
   - Geographical third-country placement of structures.

Voyage Irregularities

7. A vessel's voyage details are typically known and traceable, from departure to destination. However, since the onset of Western sanctions, Russian-affiliated ships have increasingly manipulated this information. This may be an attempt to disguise the origin of cargo, the ultimate destination, any unscheduled tours or cargo shipment through third high-risk countries. Red flags include:

   - Location manipulation - Russia has used satellite spoofing to mask the true location of a vessel(s).
   - Identify manipulation - displaying false vessel information.
   - Location misalignments and anomalous behaviours. Fake Signals.
   - Disabling AIS. A ship's Automatic Identification System (AIS) can be disabled but does not necessarily indicate illicit activity. However, repeated, prolonged, and unexplained gaps in AIS, especially in high-risk locations, should be treated sensitively.

[9] Belsat 'Gabon faces consequences for assisting Russia in the oil trade' (January 2025)

Vessel Profile

8. The shadow fleet consists predominantly of old uninsured vessels; this fleet is responsible for 70% of Russia's oil transportation, selling above the price cap threshold. The following are red flags associated with these vessels:

- Lacking P&I insurance.
- Ageing vessel.
- Lacking inspection data.
- Non-classed / non-IACS classed.

Ship-to-ship (STS) Transfer

9. STS transfers can be used to conceal the nature, origin, and destination of cargo and evade the oil price cap. Red flags include:

- Single / Chains transfers.
- Floating Storage / Blending.
- Carried out in conjunction with AIS manipulation or spoofing.
- Disregarding pre-notifications and reporting obligations.

Opaque Shipping & Ancillary Costs

10. The manipulation of ancillary and shipping costs can be used to conceal Russian oil being purchased above the price cap. If the costs are not in line with industry standards or not commercially reasonable, this may be a red flag for price cap evasion.

Indicators for Financial Sector[10]

Located in known diversionary destination	Misalignments between item / service and purchasers' line of business	Company incorporated after February 2022	Over / under invoicing
Noncooperative customers (lack / refuse to provide documentation	Common high-priority goods screening	Entities with little / no web presence	Misalignments between phone number country codes and destination countries
Name / address is similar to designated entities / individuals	Entities located at known transhipment points	Civil end users with military connections	Last-minute changes in payment routing
	Colocation / shared ownership with designated entities / individuals	Shipments going to known diversionary destinations	

[10] Jeremy Domballe, *Navigating sanctions evasion: Trade analysis of high-priority goods exports to Russia* (S&P Global Market Intelligence, 2024) p. 6

INTEL INSIGHT intelligence insight

Financial Intelligence Unit - Jersey

APPENDIX 1

ATTENTION

FIU Intelligence - Report Handling Instructions

This FIU report may contain highly sensitive intelligence and personal data. It is provided in confidence. Misuse of this report or the data contained within it may constitute an offence under the OFFICIAL SECRETS (JERSEY) LAW 1952; the OFFICIAL SECRETS ACT 1989 and/or the NATIONAL SECURITY ACT 2023. This report aligns to UK definitions. It is distributed to such persons only as needs to know its contents in the course of their official duties. It may be disseminated beyond the recipient with the following caveats:

1. It is to be handled in accordance with its **OFFICIAL-SENSITIVE** security classification (or higher) stipulated under the Government of Jersey Policy as amended from time to time.
2. It is shared for legitimate law enforcement or **OFFICIAL** purposes.
3. The original recipient is responsible for compliance with these instructions and is responsible for ensuring that the contents of the report are disclosed only to persons authorised by the FIU.
4. It is to be stored, accounted for, shared and destroyed in accord with relevant procedures and applicable law including that relating specifically to personal data, if applicable.
5. Every actual or potential compromise of the data, including any personal data breach, is to be reported to the FIU immediately. The FIU is to be consulted before any individual whose rights or freedoms might be affected by the breach, is informed.
6. The information is for INTELLIGENCE USE ONLY and not to be used evidentially.
7. Data within FIU reports is covered by an absolute exemption from disclosure under the Freedom of Information and Data Protection legislation. Any disclosure request or related request is to be raised to Director FIU.
8. This report may contain sensitive material as defined by the Attorney General's guidelines for the disclosure of unused material to the defence in criminal proceedings and is therefore subject to the concept of Public Interest immunity. No part of this report is to be disclosed to the defence without prior consultation with the FIU.

Classifications & Caveats

OFFICIAL - All information that is created or processed by the FIU is OFFICIAL by default, unless it is classified at a higher level. The majority of FIU information is classified at OFFICIAL and many users will work only at the OFFICIAL tier. The need-to-know principle underpins decision making on OFFICIAL information. The information creator is responsible for determining whether a recipient needs-to-know; access to OFFICIAL information should always be no wider than is deemed necessary for business needs and be risk-based.

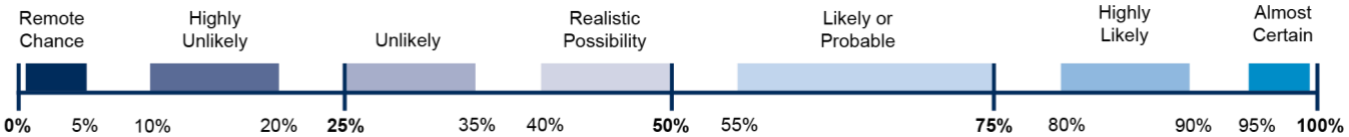
OFFICIAL-SENSITIVE - Within the OFFICIAL tier, information or material whose compromise is likely to cause damage to the work or reputation of the FIU and/or the Government of Jersey must be marked with the -SENSITIVE marking. OFFICIAL information that uses the -SENSITIVE marking may be subject to additional controls to protect need-to-know.

SECRET - Very sensitive information that requires enhanced protective controls, including the use of secure networks on secured dedicated physical infrastructure and appropriately defined and implemented boundary security controls, suitable to defend against highly capable and determined threat actors, whereby a compromise could threaten life (an individual or group), seriously damage Jersey's security and/or international relations, its financial security/stability or impede its ability to investigate serious and organised crime.

For Intelligence Purposes Only - (FOI Exempt) - This caveat means that information provided in this report can only be used for intelligence purposes only. Because of information contained, which maybe sensitive or used in pro-active investigations by other agencies, this report is exempt from any Freedom of Information requests.

Probability Yardstick

Within this document, the Professional Head of Intelligence 'Probability Yardstick' language is used and splits the probability scale into seven ranges. The below terms are assigned to each probability range. Most intelligence judgements have some degree of uncertainty associated with them. The intelligence assessment community use terms such as 'unlikely' or 'probable' to convey this. These terms are used instead of numerical probabilities (e.g. 55%) to avoid interpretation of judgements as being overly precise, as most intelligence judgements are not based on quantitative data.



Source Grading

Judging the credibility of the information provider informs the weighting applied to it during the Analysis and Assessment stage. Sources can be evaluated using the NATO-originated scales of reliability and validity: A-F/1-6.

Reliability of source	
A	Completely Reliable
B	Usually Reliable
C	Fairly Reliable
D	Not Usually Reliable
E	Unreliable
F	Reliability Cannot Be Judged

Credibility of the information	
1	Confirmed
2	Probably True
3	Possibly True
4	Doubtfully True
5	Improbable Report
6	Truth Cannot Be Judged

Confidence Levels

Confidence levels in intelligence indicate the level of certainty about an assessment. There are three levels of analytic confidence:

High Confidence	The assessment is based on high-quality information from multiple sources, and there is minimal conflict among the sources.
Moderate Confidence	The information is credible and plausible, but not of sufficient quality or corroboration to warrant a higher level of confidence.
Low Confidence	The information is questionable or implausible, or the information is too fragmented or poorly corroborated to make solid analytic inferences.

Confidence levels are more general than Probability terms. They communicate the quality of supporting information and are associated with information credibility, source reliability, correlation, and number of collection capabilities utilised. NATO members and external partners use the NATO Allied Joint Doctrine for Intelligence Procedures (NATO AJP-2.1) to communicate confidence.

Alert Category

Every intelligence report is assessed at the time of production, and an alert category status is assigned which corresponds to the category colour below. Each category status, determines the threat level warning and any possible actions that maybe required by the receiver. The levels and messaging are shown on the coversheet of reports and throughout in the header.

Alert Colour	Purpose	Alert Messaging
GREEN ALERT >	Information / Awareness	This GREEN Alert report is produced for the purposes of sharing information, training or general awareness. It should be used widely by distributed stakeholders, and it is recommended you use this Alert to complement existing knowledge and support ongoing improvements to business protocols.
AMBER ALERT >	Potential Threat / Suggest Mitigations	This AMBER Alert report is produced for awareness of potential financial crime threats with potential mitigations. This should be used to drive individual risk and threat understanding and drive potential mitigation.
RED ALERT>	Specific / Immediate Threat – Recommended Actions	This RED Alert report is produced for immediate or specific high impact threats with suggested actions. We recommend this Alert supports wider mitigations across businesses.