National Crime Agency

Joint Money Laundering Intelligence Taskforce | NATIONAL ECONOMIC CRIME CENTRE

Office of Financial Sanctions Implementation HM Treasury | Foreign, Commonwealth & Development Office

Red ALERT

Shadow Fleet Sanctions Evasion and Avoidance Network

Date: July 2025

Reference: 0774-NECC

This Red Alert is issued by the United Kingdom's National Crime Agency (NCA), a member of the National Economic Crime Centre (NECC), and HM Treasury's Office of Financial Sanctions Implementation (OFSI), working in conjunction with law enforcement and financial sector partners as part of the Joint Money Laundering Intelligence Taskforce (JMLIT+). The JMLIT+ was established to ensure a more collaborative approach between law enforcement and the banking sector.

This alert is devised with the aim of promoting awareness and bringing about preventative action. We recommend you use this Alert to complement existing knowledge and support ongoing improvements to your business processes and procedures.

This information is for your immediate attention.

Overview

This JMLIT+ Red Alert is jointly issued by the National Crime Agency (NCA), Office of Financial Sanctions Implementation (OFSI), and Foreign Commonwealth & Development Office (FCDO). The purpose of the alert is to provide information to assist financial institutions in identifying potential sanctions evasion in relation to the sale of Russian oil and gas.

What We Would Like You to Do

The National Crime Agency (NCA) is a national law-enforcement agency which leads the UK's fight to cut serious and organised crime. The NCA Alerts process is the way in which we provide information to non-law enforcement bodies including the private sector to combat and disrupt serious crime. To help us to improve this service, we would welcome any feedback you have on both the Alert itself and the information provided to you. Please email all feedback to NECC.PPP@nca.gov.uk and include the reference 0774-NECC in the subject line.

If you identify activity which may be indicative of the activity detailed in this report, and your business falls under the regulated sector, you may wish to make a Suspicious Activity Report [SAR]. If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help our analysis if you would include XXJMLXX within the text and the reference 0774-NECC for this alert within the relevant field on the NCA SAR Portal.

The NCA would also welcome any information identified as a result of this alert which does not constitute a SAR. Please email all such information to NECC.PPP@nca.gov.uk. Any information received in this way will be treated in confidence and will be handled in line with the data protection principles.

HM Treasury's Office of Financial Sanctions Implementation (OFSI) is the UK's competent authority for the implementation of financial sanctions. If you identify information that is indicative of either a frozen asset or of a breach of financial sanctions, such as dealing with frozen assets or funds involving a designated person, then you must report this to OFSI. Please email all such information to OFSI@hmtreasury.gov.uk. OFSI is also the UK's competent authority responsible for the implementation of the UK's ban on the maritime transportation of Russian oil and oil products and associated services, including civil enforcement of related breaches. If you identify information that is indicative of a breach of regulations and the Oil Price Cap (OPC) then you must report this to OFSI. Please email all such information to oilpricecap.ofsi@hmtreasury.gov.uk.

Background

Russian energy exports are funding their war in Ukraine. In 2024, 30% of Russia's federal budget came from oil and gas sales. Russian oil trading companies are utilising a complex network of companies to evade sanctions whilst accessing Western finance and professional services in order to continue to fund the Russian state.

In 2024, a network of companies run by UK-sanctioned Azeris Etibar EYYUB and Tahir GARAYEV[1] traded more Russian oil than any other entity. This included the majority of ROSNEFT's oil. EYYUB and GARAYEV themselves have personal relationships with UK-sanctioned ROSNEFT CEO Igor SECHIN which enables this privileged access to Russia's largest state-owned oil company.

Russian Sanctions Evasion and Avoidance Network

The sanctions evasion and avoidance network is resilient and consciously split between two sides, and known to its affiliated traders/brokers as "blue" and "red". The "blue" side works with entities in the Global West, including banks, insurers and trading platforms. The leading companies of this side of the network were 2RIVERS DMCC and 2RIVERS PTE, both sanctioned by the UK in December 2024. The "red" side of the network, with deliberately obscure ownership structures and many front companies designed to be replaced with ease if they are subject to Western sanctions, trades Russian oil directly. The leading company on this side of the network was NORD AXIS, sanctioned by the UK in May 2025.

Finance and oil move between the different sides of the network. Access to Western rates of trade finance, trusted insurers and key commodity exchanges utilised by 'blue' companies are combined with the special relationship with ROSNEFT's CEO and privileged access to Russian oil of the 'red' companies, to create a global trading network generating billions of USD. Money and oil move between the companies through transhipments of oil and mixing operations to hide the Russian origin.

The 2RIVERS network utilises over 100 Shadow Fleet oil tankers, vessels which are usually over 15 years old and use deceptive shipping practices to carry Russian oil. Deceptive practices include switching off the ship's automatic identification system (AIS) to avoid the ship's movements being tracked, engaging in ship-to-ship transfers to obscure the origin of the oil before it reaches its destination, and regularly changing flags. Over 400 Shadow Fleet vessels have now been sanctioned by the UK, EU, US and Canada.

[1] https://assets.publishing.service.gov.uk/media/681d97c79ef97b58cce3e615/Notice_Russia_090525.pdf

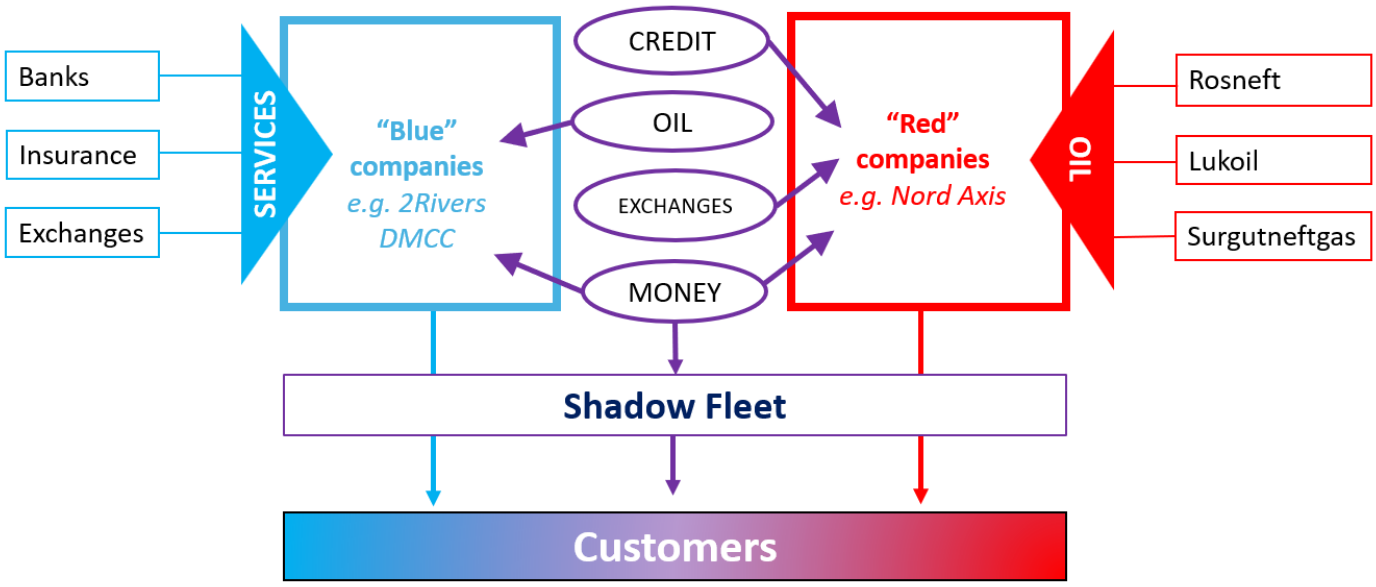

Figure 1. Diagram of how the Blue and Red companies interact with Western finances

Example:
Oil may be purchased from ROSNEFT by a company registered in a high-risk jurisdiction. This company moves it on a Shadow Fleet vessel to a terminal in a third-party location, the refined product is "sold" to another company within the same network which then sells the oil on the open market to the ultimate customer who may have no sight of its Russian origins. In this example, the first company will likely be on the "red" side of the network and the second company on the "blue". This "blue" company is able to benefit from all of the Western services but still acquire and sell Russian oil at favourable prices. Each trade carried out by the network will differ depending on the source of the oil, oil product, end customer and market conditions but often there will be a red-blue interaction (or multiple interactions) somewhere in the trading chain.

The sanctions on 2RIVERS DMCC and 2RIVERS PTE will have severely limited the network's ability to access Western services and trade Russian oil profitably. However, there are many more companies within this network, and the people behind it will likely continue to attempt to manipulate the system to benefit their trade by replacing sanctioned entities with freshly incorporated companies clean of sanctions but fulfilling the same role.

We are raising awareness of these malicious practices in order for Western banking, insurance and the professional service industry to be alert to the persistent attempts employed by the people and companies associated with EYYUB and GARAYEV and to help keep up the pressure on this network.

The Russian Federation's use of this identified sanctions evasion and avoidance scheme is unlikely to be isolated to ROSNEFT only[2].

Red Flag Indicators

No single red flag is necessarily indicative of illicit or suspicious activity, all the surrounding facts and circumstances should be considered before determining whether a specific transaction or customer is suspicious or associated with potential sanctions evasion.

- Companies with limited trading history very quickly trading large volumes of oil;
- Limited information on ownership, directors or beneficiaries;
- Multiple transfers between obscure companies;
- Companies registered or operating in known jurisdictions of high risk, including those where shadow fleet entities are known to operate;
- The companies often have a limited online presence with no company website or contact information. If a website does exist, generally it will contain generic stock photos, and no details on the individuals operating the company.

[2] http://www.occrp.org/en/investigations/in-false-transit-loophole-russias-war-machine-is-supplied-through-kazakh-companies-and-belarusian-warehouses

Data Protection Act and UK General Data Protection Regulation (UK GDPR)

The NCA reminds you of your legal obligations in respect of the management of this information, including under the Data Protection Act 2018 and the UK GDPR.

Article 5(1) of the UK GDPR requires that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner;

2. Collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with these purposes;

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. Accurate and where necessary kept up to date;

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6. Processed in a manner that ensures appropriate security of the personal data.

In addition to the general principles above, there is a possibility, given the nature of the work in question, that the personal data of some of those involved will include special categories of personal data such as sex life (and sexual orientation). Further requirements for processing this category of data are set out in the DPA and UK GDPR.

Suspicious Activity Reporting [SARs]

If you know or suspect that there has been money laundering or terrorist financing activity (including as a result of information provided to you by the NCA) and your business falls within the regulated sector, then you are reminded of the obligations to make reports to the NCA under Part 7 Proceeds of Crime Act 2002 and the Terrorism Act 2000. If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help our analysis if you would include the reference 0774-NECC within the specified field on the NCA Portal. This reference is specific to the Alerts process; where appropriate, we would ask that this is used *in addition* to the ongoing use of the Glossary Codes. Guidance on making suspicious activity reports is available at www.nationalcrimeagency.gov.uk.

Disclaimer

While every effort is made to ensure the accuracy of any information or other material contained in or associated with this document, it is provided on the basis that the NCA and its staff, either individually or collectively, accept no responsibility for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any such information or material.

Any use by you or by any third party of information or other material contained in or associated with this document signifies agreement by you or them to these conditions.

Alert Markings

NCA Alerts are marked either Red or Amber. This is designed to indicate the urgency of the warning. Red may indicate a more immediate or specific threat, whilst those marked Amber will provide more general information that may complement existing knowledge.

NCA Alerts Team

Recognising that the private sector is often the victim of serious organised crime and is engaged in its own efforts to prevent, deter, and frustrate criminal activity, the NCA seeks to forge new relationships with business and commerce that will be to our mutual benefit – and to the criminals' cost. By issuing Alerts that warn of criminal dangers and threats, NCA seeks to arm the private sector with information and advice it can use to protect itself and the public. For further information about this NCA Alert, please contact the NCA Alerts team by email alerts@nca.gov.uk. For more information about the National Crime Agency go to www.nationalcrimeagency.gov.uk.

Protecting the Public – Providing Information Back to the NCA

Section 7(1) of the Crime and Courts Act 2013 allows you to disclose information to the NCA, provided the disclosure is made for the purposes of discharging the NCA's functions of combating serious, organised, and other kinds of crime. The disclosure of such information to the NCA will not breach any obligation of confidence you may owe to a third party or any other restrictions (however imposed) on the disclosure of this information. The disclosure of personal information about a living individual by you to the NCA must still comply with the provisions of the Data Protection Act 2018 (DPA). However, you may be satisfied that the disclosure by you of such personal information to the NCA in order to assist the NCA in carrying out its functions may be permitted by Schedule 2, Part 1 of the DPA 2018. This allows a data controller to be exempt (by means of a restriction or adaption) from provisions of the GDPR, if the personal data is processed for the following purposes:

a) the prevention or detection of crime,
b) the apprehension or prosecution of offenders, or
c) the assessment or collection of a tax or duty or an imposition of a similar nature,

to the extent that the application of those provisions of the GDPR would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).
(DPA 2018, Schedule 2, Part 1).

Any Section 7(1) information should be submitted to alerts@nca.gov.uk.

The NCA's Information Charter is published on our external website at www.nationalcrimeagency.gov.uk.

Handling Advice – Legal Information

This information is supplied by the UK's NCA under Section 7(4) of the Crime and Courts Act 2013. It is exempt from disclosure under the Freedom of Information Act 2000. It may be subject to exemptions under other UK legislation. Except where permitted by any accompanying handling instructions, this information must not be further disclosed without the NCA's prior consent, pursuant to schedule 7, Part 3, of the Crime and Courts Act 2013.

This report may contain 'Sensitive Material' as defined in the Attorney General's guidelines for the disclosure of 'Unused Material' to the defence. Any sensitive material contained in this report may be subject to the concept of

Public Interest Immunity. No part of this report should be disclosed to the defence without prior consultation with the originator.

Requests for further disclosure which are not permitted by any handling instructions or handling code must be referred to the NCA originator from whom you received this information, save that requests for disclosure to third parties under the provisions of the Data Protection Act 2018 or the Freedom of Information Act 2000 and equivalent legislation must be referred to the NCA's Statutory Disclosure Team by e-mail on statutorydisclosureteam@nca.gov.uk.