National Crime Agency

NECC
NATIONAL ECONOMIC CRIME CENTRE

10 YEARS
PUBLIC PRIVATE PARTNERSHIPS

Office of Financial Sanctions Implementation
HM Treasury

Foreign, Commonwealth & Development Office

Networks & Shadow Fleets

Date: November 2025

Reference: 0788-NECC

This Amber Alert is issued by the United Kingdom's National Crime Agency (NCA), a member of the National Economic Crime Centre (NECC), 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.

AMBER ALERT

Overview

This JMLIT Alert is jointly issued by the National Crime Agency (NCA), Office of Financial Sanctions Implementation (OFSI), and Foreign Commonwealth & Development Office (FCDO). The alert is intended to raise awareness and share information, helping maritime and financial institutions identify and prevent sanctions evasion involving commodities and financial transactions by networks and shadow fleets that support sanctioned regimes.

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 0788-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 0788-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, including any information on action taken by you which you believe has or could have a disruptive impact on serious organised crime. 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 sanctioned products and associated services, including civil enforcement of related breaches. If you identify information that is indicative of a breach of regulations then you must report this to OFSI. Please email all such information to ofsi@hmtreasury.gov.uk

Background

Sophisticated, state-backed networks support the sanctions evasion strategies of regimes like Russia, Iran and the Democratic People's Republic of Korea (DPRK) by exploiting: opaque corporate structures, covert financial systems and deceptive maritime practices to further their illicit activities. These regimes have developed highly organised and adaptive mechanisms to evade sanctions, enabling them to continue generating critical revenue streams from energy commodities, despite heavy international scrutiny.

Expanding on Alert 0774-NECC Shadow Fleet Sanctions Evasion and Avoidance Network, this Alert explores similar networks, and examines the shadow fleets that are enabling circumvention on behalf of Russia and other regimes, the methods and people they employ, and the sanctions and money laundering typologies that can be used to help detect these operations.

Regime Sustainment

Some sanctioned regimes, such as Russia and Iran, rely on commodity export revenues to fund state expenditure and sustain elite networks. While Russia's energy income supports its military objectives in Ukraine, Iran uses its energy revenue to bolster its economy, advance its nuclear programme, and procure weapons and dual-use technologies.

Russia generated around USD 120.5 billion in energy (oil and gas) revenue in 2024, representing about 30% of state revenue[1], some of which was supplied to the DPRK.[2] Meanwhile, energy revenue is projected to account for approximately 35.1% of Iran's 2025 national budget, amounting to an estimated USD 56 billion.[3] In response, aligned sanction authorities have introduced increasingly targeted measures, focusing on access to global financial systems, commodities, and their transportation, to constrain revenue streams. In 2025 over 180 vessels supporting Russia and other sanctioned regimes that form part of the global shadow fleet were designated by various sanctioning authorities, alongside enablers, many of which operate in third-country trading hubs.

[1] Oxford Institute for Energy Studies - Vitaly Yermakov, "Fiscal Flex: Russia's oil and gas revenues in 2024," The Oxford Institute for Energy Studies, February 2025, https://www.oxfordenergy.org/wpcms/wp-content/uploads/2025/02/Comment-Fiscal-Flex.pdf. & C4ADS – Oil Water report

[2] BBC News – Satellite Images Show Russia Giving N Korea oil, breaking Sanctions – 21 Nov 2024

[3] Oxford Institute for Energy Studies - Vitaly Yermakov, "Fiscal Flex: Russia's oil and gas revenues in 2024," The Oxford Institute for Energy Studies, February 2025, https://www.oxfordenergy.org/wpcms/wp-content/uploads/2025/02/Comment-Fiscal-Flex.pdf. & C4ADS – Oil Water report

Market Access

These regimes maintain access to global markets through intricate networks of intermediaries and trusted facilitators. These networks play crucial roles in enabling illicit trade, including the movement of commodities, concealment of vessels and cargo identities, manipulation of financial transactions, falsification of documentation and the laundering of proceeds. In return, these facilitators often receive preferential consideration, significant financial rewards, trade access or protection from in-country (regime) scrutiny.

These commodity trading networks have shown significant skill in navigating and employing complex facilitation structures. They utilise front companies and reflagged ageing vessels, often leveraging European and North American financial systems and professional services.

Evasion Networks

EXAMPLE 1: Network & Sanctions

A network, associated to Hossein SHAMKHANI (a.k.a. Hector SHAMKHANI, Mohammad Hossein SHAMKHANI)[4], himself UK, EU, US sanctioned, and the son of US-sanctioned Ali SHAMKHANI[5], leverages a web of shipping companies, financial intermediaries, and firms linked to sanctions. Originally established as a family-run shipping venture it expanded rapidly, and aligned with the interests of sanctioned regimes.

It controls numerous entities, including MILAVOS GROUP[6], (UK, EU sanctioned) and OCEAN LEONID INVESTMENTS[7] (UK, US sanctioned). These entities operate in shipping, petrochemicals, and finance.

Shadow Fleets

As sanctions resulted in isolation from some markets, Russia and Iran have turned to evasion networks, selling commodities such as oil and gas to countries willing to buy at discounted rates. As a result, a parallel market emerged, enabled by these networks and their maritime logistics. In 2023, all of one regime's crude oil exports were transported by sea, highlighting the maritime sector's pivotal role in sustaining sanction circumvention networks.[8]

The use of so-called 'shadow', 'ghost', or 'dark' fleets has become systematic. The shadow fleets primarily consist of older vessels, estimated between 700 to 1000 in number[9], with opaque ownership structures. These ships are routinely renamed, reflagged under permissive jurisdictions and insured through shell entities.

[4] OFSI Consolidated sanctions listing Group ID 17041 & https://home.treasury.gov/news/press-releases/sb0215 /
[5] Typology Analysis, & OFAC sanctions listing, Iran-EO13876 SDN
[6] Typology Analysis & OFSI Consolidated sanctions listing Group ID 17044
[7] OFSI Consolidated sanctions listing Group ID 17043
[8] C4ADS Oil Water.
[9] C4ADS Oil Water.

Vessels' Automatic Identification System (AIS) transponders are frequently disabled or obscured using techniques such as signal spoofing, particularly in critical maritime areas including the Persian Gulf, Gulf of Oman, and the Baltic and Barents Seas. This practice conceals voyage data, and violates international maritime safety conventions. AIS technology is designed to continuously transmit a vessel's identity and location to prevent collisions at sea. Its manipulation increases the risk of accidents, and environmental disasters and undermines regulatory oversight.

Evasion Networks

EXAMPLE 2: Network with Shadow Fleet for Hire

Based on aggregated open source[10] and feedback from public sector stakeholders' - since 2019, a shadow fleet network has strategically acquired tankers and put them to work transporting commodities (crude oil) from heavily sanctioned states. This network's fleet is responsible for under 10% of the total of Shadow Fleet operations. It operates under multiple false flags, and uses Ship-To-Ship (STS) transfers and secret storage facilities to mask the origin and destination of its cargo. These operations have enabled the covert movement of hundreds of millions of barrels of sanctioned crude oil into global markets since 2019.

Financially, the network has leveraged its vessels as collateral for hundreds of millions of dollars in loans from opaque financial institutions based in offshore jurisdictions. This activity depends on a web of offshore shell companies and sophisticated laundering techniques, including cryptocurrency transactions, to process and conceal profits. Estimates suggest the operation generates over USD $15 billion annually and moves approximately 1 million barrels of oil per day.

In 2022, with at least 25 vessels under its control, it seamlessly shifted to carrying Russian oil in the wake of sanctions triggered by the invasion of Ukraine. This built-in adaptability makes this network's fleet, and similar sub fleets, indispensable tools for sanctioned regimes, by being able to swiftly redirect their assets to serve any nation seeking to bypass international restrictions.

The use of circuitous maritime routes and fabricated paperwork can also seek to disguise sanctioned shipments as legitimate. Common destinations for these disguised energy commodities include Southeast Asia, the Arabian Gulf and the Indian Ocean via the Mediterranean.

The transport of commodities via these routes often involve shadow fleet tactics that rely on a chain of intermediaries and forged documentation. Port call records are frequently missing or manipulated, to mask shipment origin and destination. To further obscure the origin of

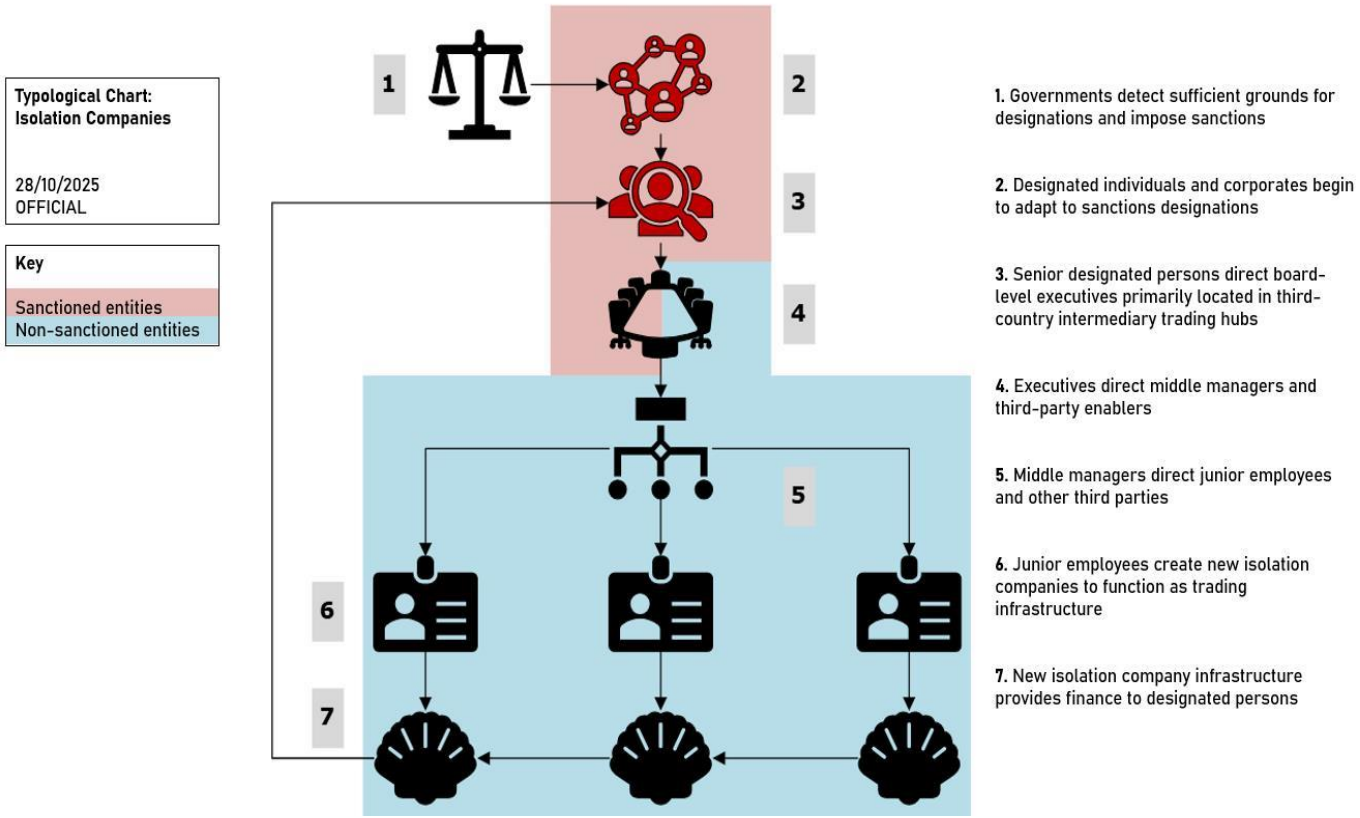
[10] C4ADS Oil Water.

sanctioned commodities, networks engage in blending and co-mingling tactics, where sanctioned cargo is mixed with legitimate product during offshore ship-to-ship transfers. Such operations are frequently carried out in loosely regulated maritime zones, to reduce detection.

Front Companies

The use of front or shell companies is also central to these operations. Entities are often incorporated in jurisdictions with limited corporate transparency and may lack any financial history or ongoing business activity. In more elaborate schemes, front companies are registered in reputable financial centres, with ostensibly plausible business operations and financial activity, which raise few immediate suspicions. In reality, however, their behaviour far exceeds normal business patterns and knowledge of its corporate members.

Financial flows connected to these networks are similarly complex. Transactions are routed through non-transparent intermediary structures, shell companies, or isolation companies. In many cases, payments are conducted via barter, alternative currencies or digital assets to avoid detection through financial institutions. Trade documents frequently misrepresent the origin of cargo, even when maritime data clearly traces the shipment to sanctioned ports. These methods are complemented by complex corporate structuring and the use of deceptive shipping practices. Facilitators often possess expertise in offshore finance, informal value transfer systems (IVTS) and regulatory loopholes, allowing them to operate without detection.



Network Typology Characteristics

The networks supporting shadow fleet activities span a range of typologies (see table below) that are frequently used in combination, to reduce detection. Typologies may pass undetected in isolation, but when several appear together, they form a pattern. Networks like those in the examples above design systems using enablers, environments and several indicators simultaneously, across webs of shell entities, jurisdictions, individuals, and operations.

Network Typology Characteristics	Summary
Shipping: Use of Illicit Vessels	Use of disguised vessels, ageing and poorly maintained vessels, and registries/flags from low due diligence jurisdictions.
Shipping: Obfuscation	Disguising illicit shipments using documentation fraud, illicit Automatic Identification System (AIS) activity, or impersonating other vessels.
Shipping: Successive Ship-to-Ship Transfers	Multiple use of ship-to-ship transfers to obfuscate the transportation of goods.
Company Incorporation	Entities registered in jurisdictions of interest.
Extensive Use of Isolation Companies	Establishment of numerous entities, compartmentalised with minimal footprint used in tandem.
Unusually Rapid Commercial Expansion	Fast entry and scaling in high-risk sectors without logic or prior experience.
Obfuscated Corporate Restructuring	Frequent changes in company ownership, structure, or control to obscure beneficial ownership and trust purpose. This includes frequent creation of new companies within structures.
Heavy reliance on serviced office addresses, for claimed international addresses	Use of virtual offices or service providers to establish international presence without actual operations and/or to acquire access to reputable financial services.
Jurisdictional Gaming and Duplicate Incorporation	Similarly-named entities spread across multiple jurisdictions.
Exploitation of Brand Reputation	Use of names resembling reputable brands to benefit from false legitimacy.
Random or Meaningless Company Names	Use of nonsensical or generic names without contextual logic.
Mismatch between Senior Role and Limited Experience	Individuals in high-ranking positions lacking requisite experience or credibility.
Overlapping Employer/Employee Relationships	Individuals appear in contradictory roles, or holding multiple roles across related entities, blurring lines.

Employer and Employee Obfuscation	Lack of transparent roles, titles, job function, and employment relationships.
Citizenship by Investment	Individuals hold passports from tax havens or permissive jurisdictions.
Unsubstantiated Commercial Capabilities	Claims of infrastructure, expertise, capacity without supporting evidence or track record.
Commercial Associations with Opaque Entities	Partnerships/relationships with questionable or unverified organisations.
Dubious or Superficial Website Presence	Basic websites with vague content, no individual identifiers, over use of confidential clauses and, exaggerated credentials. Contact information and limited online presence lacking substance.
Telephone Number Irregularities	Sharing or untraceable phone contacts across entities.
Use of Consumer Email	Use of free domains for corporate communications and activities.
Misleading Addresses	Prestigious addresses without physical offices.
Inconsistent or Varied Name Spellings	Minor or frequent name discrepancies across platforms to complicate automated transaction screening.
Flaunting of Wealth	Visible affluence within sectors not aligned with commercial success.
Association with High-Profile Figures	Cited relationships that are designed to create a veneer of legitimacy, and credibility but lack substance or evidence.
Affiliation with International Bodies	Misrepresented memberships or recognitions.
Politically Exposed Persons (PEPs) Using Family Proxies to manage affairs	Relatives of high-risk PEPs almost certainly use family members in business roles.
Spousal or Proxy Ownership	Spouses or proxies listed with no qualifications or background.
Questionable Academic Qualifications	Unverifiable education credentials, of those involved in the networks.
Honorary or Purchased Titles	Adoption/use of misleading honorifics to feign legitimacy and project credibility.

Combined Typologies of the Networks

The networks often deploy all or many of these characteristics simultaneously within their activities. The interlinking of multiple characteristics adds exponential complexity to illicit networks.

- Network Camouflage: Every new layer (person, company, title) by networks aids concealment.
- Legitimacy Illusion: Use of international affiliations, misleading addresses, and titles creates trust.
- Systemic Difference Exploitation: Differing jurisdictional thresholds are exploited, to support networks objectives.

Examples of Combined Typologies of the Networks

Shipping Obfuscation + Complex Entity Structures + Isolation Companies + High-Risk Jurisdictions – Obfuscation of vessel identities (e.g. AIS spoofing), paired with complex, multi-jurisdictional corporate layering and use of shell entities, may signal sanctions evasion from illicit shipping.

Use of Illicit or Ageing Vessels + Registration in Low-Due-Diligence Flag States + Unsubstantiated Capabilities + High-Risk Jurisdictions + Rapid Expansion – The use of substandard vessels (poor vessel maintenance history, suspicious fleet acquisitions, fraudulent documents, and regular name changes), particularly under flags of convenience (flag hopping), combined with entities that grow rapidly without a commercial track record, may signal concealment activities or front operations.

Fake or Prestigious Office Locations + Shell Companies + Trust and Company Service Provider's Address + Proxy Ownership + Purchased Titles + Misleading Website + Isolation Companies - May signal that entities are constructing an illusion of legitimacy or international scale without a physical presence, and are engaged in an elaborate effort to obscure beneficial ownership, inflate credibility, and access financial channels.

Red Flag Indicators

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

The presence of one or more indicators does not confirm wrongdoing but may require further review.

Vessels:

- Shipping companies or consignments that have changed ownership, name, management structures or flag within a short timeframe, with no clear commercial rationale.

- Front companies incorporated in the past 12 months with no evident operational history, often sharing addresses, directors, or email domains.

- Vessels, counterparties, or cargo exhibiting sudden changes in names, flags, or corporate affiliations, particularly where linked to offshore jurisdictions.

- Maritime vessels engaged in voyages with gaps or unexplained deactivations in AIS transmissions during transits near sanctioned jurisdictions or high-risk maritime zones.

- Inconsistent cargo documentation (origin vs routing) - Bills of Lading and certificates of origin that conflict with maritime tracking or port call records.

- Routing of commodities (oil, gas, metals, petrochemicals) through trans-shipment hubs with no commercial logic, or frequent short-term anchorage.

- Entities with historic links to designated persons, leaked registries, or law enforcement reports.

- Engagement with clients, counterparties or vessels previously linked to sanctions breaches or designated persons, or law enforcement reports.

Transactions & Routings:

- Trade flows exhibiting circular routing or unnecessary complexity without a clear commercial rationale.

- Unusual or non-standard payment arrangements, including third-party payments, use of cryptocurrencies, or payment terms inconsistent with industry norms.

- Payments routed through multiple intermediaries, especially via non-transparent offshore jurisdictions.

- Payment terms that involve third parties, obscure remittance sources, crypto wallets, or currencies not typically used in global commodities markets.

- Transactions routed through banks or payment institutions known to have weak Anti-Money Laundering / Counter-Terrorism Financing controls, or where sanctions evasion cases have occurred.

- Obfuscated corporate restructuring, with frequent changes or creation in company ownership, structure, or control to obscure beneficial ownership and true purpose.

- Use of Isolation Companies - establishment of numerous entities, compartmentalised with minimal footprint of exposure to designated persons used in tandem.

- Unusually rapid commercial expansion - fast entry and scaling in high-risk sectors without logic or prior experience.

- Random or meaningless company names - use of nonsensical or generic names without contextual logic.

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 0788-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.

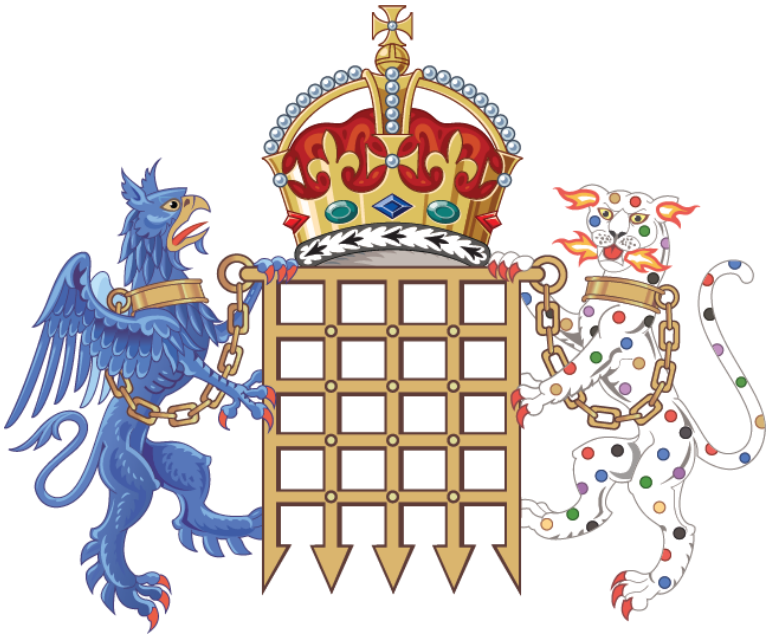
Handling Advice – Legal Information

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.



NCA
National Crime Agency

nca.gov.uk

NECC
NATIONAL ECONOMIC CRIME CENTRE

10 YEARS
PUBLIC PRIVATE PARTNERSHIPS

Follow us on LinkedIn:
@National Economic Crime Centre (NECC)