National Crime Agency

NECC

NATIONAL ECONOMIC CRIME CENTRE

jmlit

Joint Money Laundering Intelligence Taskforce

Office of Financial Sanctions Implementation HM Treasury

Red ALERT

Financial Sanctions Evasion Typologies: Russian Elites and Enablers

Date: July 2022
Reference: 0697-NECC

This Red Alert is issued by the National Economic Crime Centre (NECC), a multi-agency unit in the National Crime Agency (NCA), 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 is managed in the NECC and was established to ensure a more collaborative approach between law enforcement and the banking and wider private 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 on-going improvements to your business processes and procedures.

Overview

This alert is issued by the JMLIT+ Sanctions Facilitators Cell, with representation from law enforcement, private industry, financial crime regulators and OFSI.

For indicators of sanctions evasion, go to the following pages for the relevant sectors:

- For detection of **frozen asset transfers**, go to page 9
- For detection of **enablers**, go to page 10
- For detection of **suspicious payments**, go to page 10
- For **industry recommendations**, go to page 11

The purpose of the alert is to provide information from law enforcement and the legal and financial services sectors as to some common techniques designated persons (DPs) and their UK enablers are suspected to be using to evade financial sanctions.

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 alerts@nca.gov.uk and include the reference **0697-NECC** in the subject line.

If you identify activity which may be indicative of the typology 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 **0697-NECC** for this alert.

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 jmlit@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

Information Report

Executive Summary

Russian aggression in Ukraine is enabled by the elites who control Russia's economic interests. The UK, US, EU and other allies are targeting those elites with unprecedented sanctions, seeking to drive a change in behaviour from both them and from the Russian government over its invasion of Ukraine.

A priority for designation has been those corrupt elites who have obtained a benefit from the Government of Russia. These close relationships have allowed these individuals to secure and retain control over misappropriated assets.

From case studies identified through financial intelligence and other sources, some Designated Persons (DPs) are using a range of techniques in order to evade sanctions impacting on their personal and commercial holdings. While this behaviour has generally occurred prior to sanctions being imposed on the DP, it is also happening shortly afterwards. While there has been coordination between sanctions designation and implementation authorities such as the EU, the US Office of Foreign Asset Control (OFAC) and UK HM Treasury's Office of Financial Sanctions Implementation (HMT OFSI) and Foreign, Commonwealth & Development Office (FCDO), differing timescales in designating individuals between jurisdictions created opportunities for DPs to facilitate the movement of funds/assets.

DPs are using associates, including family members and close contacts, via enablers to:

1. Transfer assets such as shareholdings in holding companies to trusted proxies such as relatives or employees;

2. Sell or transfer assets at a loss in order to realise their value before sanctions take effect;

3. Divest investments to ensure ownership stakes are below the 50% threshold, or relinquishing previous controlling stakes.

Although a DP may claim to have relinquished the asset, it is highly likely that they will retain their influence through trusted proxies and enablers. Enablers are individuals or businesses facilitating sanctions evasion and associated money laundering. Facilitation requires:

i) the criminal activity not happening, or being more difficult, without the enabler;

ii) assisting a suspect to evade scrutiny by distancing the suspect in some way from the offence; and/or

iii) allowing a suspect to benefit by laundering proceeds or assisting with doing so.

Key professions include (but are not limited to) legal (barristers and solicitors), financial (relationship managers, accountants, investment advisors, wealth managers, payment processors, private equity, trust and company service providers), estate agents, auction houses, company directors, intermediaries/agents and private family offices.

The NCA and SFO have previously jointly assessed that, in relation to international bribery and corruption, London-based enablers are almost certain to be in senior positions (director, owner, CEO, senior partner) within their company or business. Enablers' level of complicity is assessed at three common levels: criminally complicit, wilfully blind (for example in relation to source of funds checks) and unwittingly involved.

Relevant Sanctions Evasion Offences

After a UK designation, where a DP seeks to move assets including in the methods outlined above, it could constitute breach offences under the UK sanctions regulations, as well as potential circumvention offences by the DP and any associates or enablers. The Sanctions & Money Laundering Act (SAMLA) 2018 has extra-territorial application, meaning it applies to all UK persons in England, Wales, Scotland, Northern Ireland, the Crown Dependencies and Overseas Territories.

Under the Russia (Sanctions) (EU Exit) Regulations 2019, there are five financial offences (regulations 11-15) that can be summarised as penalising dealing with the frozen assets of a DP and penalising making funds or economic resources (assets) available for that DP, either directly or indirectly. In addition, regulation 19 provides a circumvention offence of intentionally participating in activities knowing the object or effect is to circumvent the breach regulations or to facilitate their contravention.

This circumvention offence may apply where enablers are seeking to obstruct other parties from carrying out necessary due diligence to meet their own sanctions obligations. This could include misrepresenting entities that are owned/controlled by the DP, or by adopting overtly aggressive and litigious strategies to deflect from the DP's underlying ownership and control.

Regulation 7 offers an outline of the assets that are to be frozen. It provides for a DP's company to be frozen if any of the following conditions are met: the DP directly or indirectly holds more than 50% of shares, the DP directly or indirectly holds more than 50% of voting rights, or the DP directly or indirectly holds the right to appoint or remove a majority of the board of directors, or that the DP can directly or indirectly achieve the results of their wishes with regards to the company's affairs. Relevant firms should pay close attention to the "joint arrangements" provision in Schedule 1, by which shareholdings of a DP held in an arrangement with another person count as the combined total.

As sanctions breaches or circumvention of the regulations constitute criminal offences, this means the onward transfer of funds or assets would likely become proceeds of crime and recoverable property under the Proceeds of Crime Act 2002. This would also apply to funds transferred for an arrangement intended for use in unlawful conduct, such as a future breach or circumvention of sanctions.

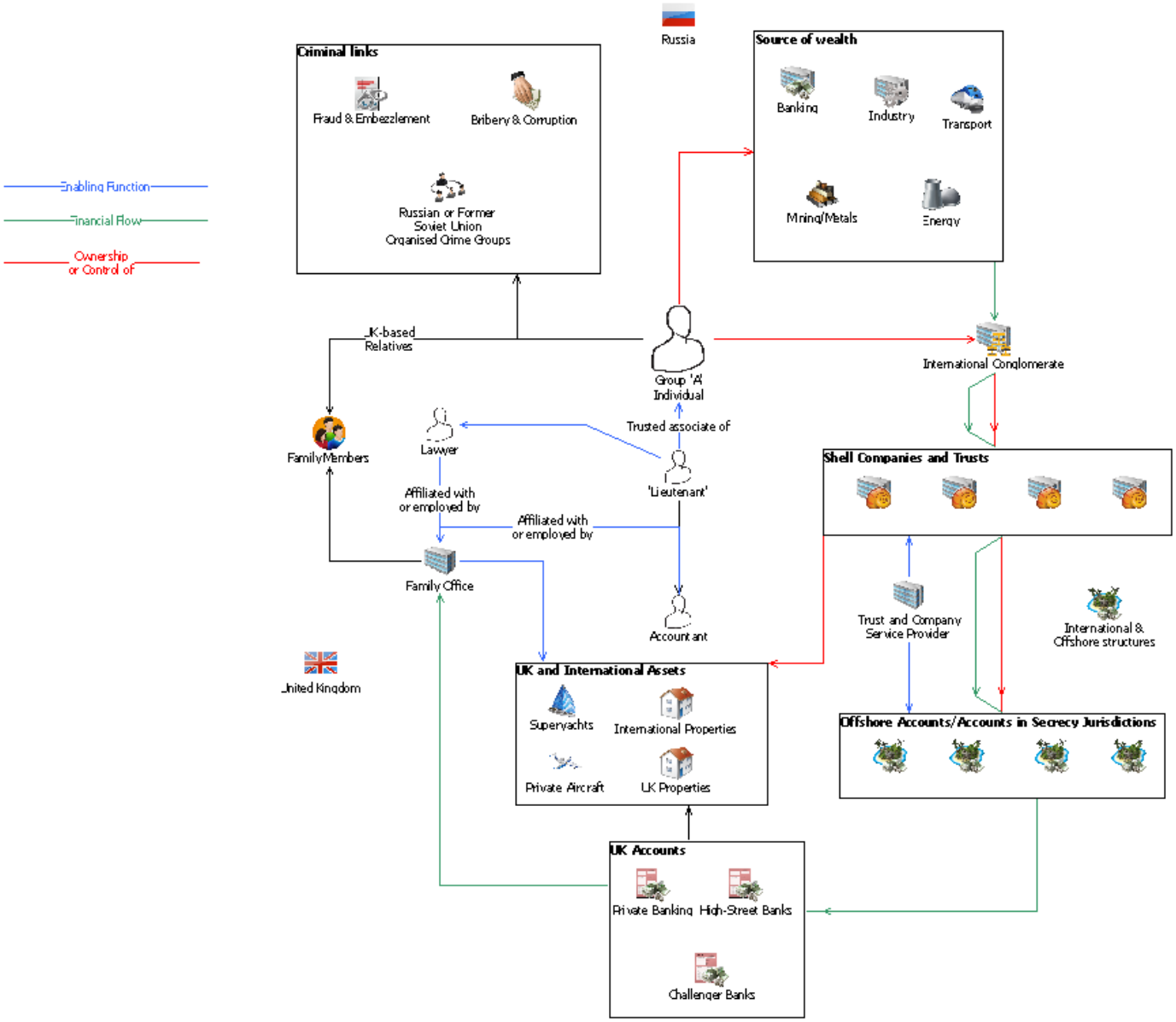
Evasion methods

DPs will seek to transfer assets and funds directly and indirectly to jurisdictions where sanctions are not in place, such as the UAE, Turkey, China, Brazil, India and the former Soviet Union (excluding the Baltic States and Ukraine). Doing so on the behalf of a DP will involve the use of multiple laundering methods, including use of secrecy jurisdictions or citing Russian legal protection from sharing information.

To move funds, it is likely that DPs will explore alternative payment methods, including the use of crypto-assets, to move funds to circumvent sanctions and mitigate reduced access to the SWIFT payment system. Russian money launderers have increasingly been observed in UK intelligence and operational activity providing cash to crypto-asset services, with the ability to move significant volumes of funds. The main barriers in upscaling crypto-asset use are liquidity and market size, while, the transparent nature of the blockchain could reduce its appeal to circumvent sanctions.

Given the unprecedented range of sanctions imposed against Russia, and the increase in activity-based sanctions targeting key industries, it is likely that certain nation-states that continue to support Russia may seek to purchase discounted oil and gas, as well as supply Russia with military hardware and other controlled goods or services. This may present opportunities for designated entities and their enablers to circumvent asset freezes.

Fig. 1: Example of a Typical Enabler Network of a Russian Ultra High Network Individual (UHNWI) or Politically Exposed Person (PEP) ("Group A Individual")



Threat Response

National Crime Agency

The NCA has surged officers into the **Combating Kleptocracy Cell (CKC)** announced by the Prime Minister in February.[1]

The CKC is:

1. targeting corrupt elites through their assets in the UK;
2. targeting key enablers of these corrupt elites;
3. identifying opportunities to strengthen cross-HMG policy and legislative defences to illicit finance; and
4. supporting criminal cross-HMG sanctions delivery and enforcement.

The CKC is multi-disciplinary, drawing on the intelligence and operational expertise of law enforcement and government partners. The focus is on corrupt elites and their enablers, against whom we will use all powers available to us to disrupt and investigate any nefarious activity. Within this, the **National Economic Crime Centre (NECC)** brokers a cross-system response from across law enforcement, regulators, government and private industry to scale up the UK's defences against illicit finance.

The UK Financial Intelligence Unit (UKFIU), also housed in the NCA, has introduced a new glossary code, **XXSNEXX** for reporters where they suspect the activity is consistent with money laundering and is linked to entities sanctioned by the UK, US, EU and other overseas jurisdictions.[2]

The NCA and NECC work particularly closely with the **Financial Conduct Authority** in relation to money laundering through crypto-assets, in order to tackle its widespread adoption by professional money launderers, including those from Russia.

Office of Financial Sanctions Implementation

HMT OFSI has issued extensive non-statutory guidance in order to support firms and members of the public in remaining compliant with financial sanctions.[3]

As a relevant firm,[4] you are legally obliged to report to OFSI if you know or suspect that a breach of financial sanctions has occurred, that a person is a DP or you hold frozen assets and that knowledge or suspicion came to you while conducting your business.

Reporting to OFSI can be delivered through the Compliance Reporting Form, which is available online:

[1] For more information, see https://www.nationalcrimeagency.gov.uk/who-we-are/publications/591-sars-in-action-march-2022

[2] https://nationalcrimeagency.gov.uk/who-we-are/publications/585-ukfiu-sar-glossary-codes-note-march-2022

[3] www.gov.uk/government/publications/financial-sanctions-faqs

[4] As defined under r71 of the Russia (Sanctions) (EU Exit) Regulations 2019

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776805/compliance_reporting_form.docx

The full list of designated persons subject to financial sanctions can be found on OFSI's consolidated list of asset freeze targets:

- https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets

To stay up to date with the latest information on financial sanctions including amendments to the consolidated list of asset freeze targets, you can subscribe to OFSI's free email alert service:

- https://public.govdelivery.com/accounts/UKHMTREAS/subscriber/new

Professional Body Supervision

As an anti-money laundering supervisor, **HMRC** is committed to helping businesses protect themselves from money laundering and terrorist financing. To help its supervised businesses be aware of and comply with their obligations, HMRC have sent several emails to businesses relating to sanctions, including considerations to make when transacting with Russia and signposts to webinars and guidance for further information.

HMRC's supervised businesses are obligated to screen against UK sanctions, the OFSI lists, and to report any knowledge of breaches. Breaches of financial sanctions are criminal offences. HMRC's supervised businesses should have adequate policies, controls and procedures in place to effectively identify and mitigate risks the business faces, including appropriately identifying and dealing with sanctioned entities. Guidance on who is subject to sanctions is on GOV.UK.

Registered businesses who fail to comply with the Money Laundering Regulations leave themselves, and the UK economy, open to attacks by these criminals. HMRC uses a wide range of measures to tackle those who breach the regulations, including civil penalties and criminal prosecutions.

Financial crime supervisors for the legal sector such as the **Solicitors Regulation Authority (SRA)** have issued various communications to the firms they regulate about the impact of Russia sanctions.[5] The conduct of law firms is expected to balance obligations to clients with duties to the public interest and the court system.[6]

In line with their anti-money laundering obligations and the application of a risk-based approach, law firms must identify and verify their clients and should obtain robust documentary evidence of their source of funds and source of wealth for their high-risk clients and matters. These checks can also help firms to limit their exposure to designated persons and frozen assets.

Wilful blindness with regards to Know Your Customer documentation in relation to high-risk customers will not be tolerated and will be considered a matter for criminal prosecution.

If a member of the public believes that a law firm has broken the rules, it can be reported to the relevant regulator, which in England and Wales is the SRA for solicitors and their firms and the **Bar Standards Board** for barristers. Further guidance on reporting is available at:

- www.sra.org.uk/consumers/problems/report-solicitor
- www.barstandardsboard.org.uk/for-the-public/reporting-concerns.html

[5] https://www.sra.org.uk/home/hot-topics/impacts-russia/

[6] https://www.sra.org.uk/solicitors/guidance/conduct-disputes/

The **Institute for Chartered Accountants for England & Wales (ICAEW)** supports the highest professional standards in accountancy practice through its Practice Assurance scheme and robust anti-money laundering supervision and monitoring. The ICAEW's regulatory response to the impact of Russian sanctions is three-fold:

- Embedded – ICAEW's proactive risk-based approach includes risk assessing firms for AML risk relating to sanctions, as well understanding the firm's assessment and compliance with sanctions through regular monitoring reviews. It conducts over 1,000 assessments a year and its 2021 thematic review covered how firms sanction-check clients.

- Enhanced – Its newly created Ukraine hub collates education and guidance on risks and how to comply with sanctions, including new guidance on sanctions to the accountancy sector. It publicises these materials through regular articles to members (both in business and practice). It has updated its monitoring work-programmes to enhance its focus on sanctions compliance.

- Accelerated – It will bring forward a scheduled thematic review for the largest firms on how they identify, handle and mitigate the AML risk associated with PEPs and sanctions. It will extend the thematic review to assess how firms identified, and managed, the AML risks associated with sanctions during this period of significant and rapid change. It will continue to assess, and communicate, to firms the emerging threats and trends.

Members of the public can raise concerns of sanctions non-compliance, or make a complaint about any other non-compliance, via their website:

- www.icaew.com/regulation/complaints-process/make-a-complaint

The **Chartered Institute for Legal Executives (CILEX)** has issued communications to its regulated firms about the impacts of Russia sanctions and the requirements to obtain licences. It has questioned firms on their understanding of, and engagement with, the sanctions guidance, and whether they are exposed to risks from carrying out work for sanctioned individuals or entities.

In addition, it has raised the issues of sanctions with all CILEX members, many of whom will work in firms and organisations regulated by other bodies. A new webpage has been created to provide greater prominence on Financial sanctions and licencing.

- https://cilexregulation.org.uk/financial-sanctions/

Within the accountancy and consultancy sectors, the **Chartered Institute of Management Accountants (CIMA)** has contacted all regulated members advising them of their obligations under the sanctions regimes relating to Russia and Belarus. To mitigate the risk of sanctions evasion by DPs, members have been reminded of the need to have robust due diligence processes in place, to review their internal risk assessments, policies and procedures and to know their clients and source of wealth. As professional accountants CIMA members are bound by a Code of Ethics which includes complying with relevant laws and regulations and acting with integrity. Failure to meet their ethical and legal obligations will result in disciplinary action being taken by CIMA.

- www.cimaglobal.com/Professionalism/Ethics/CIMA-code-of-ethics-for-professional-accountants/

- www.cimaglobal.com/Professionalism/Conduct/

The **Chartered Institute of Taxation (CIOT)** and **Association of Taxation Technicians (ATT)** have written to all AML supervised firms to raise awareness of Russian Sanctions and the importance of sanctions checks as part of the AML risk based approach. The issues have also been covered in a Professional Standards update webinar made available in May 2022. Firms are required to meet

legal requirements placed upon them and where firms fail to meet sanctions requirements, they will be referred to the independent Taxation Disciplinary Board. Information about Russian Sanctions has been made available via the following website pages:

- www.tax.org.uk/new-financial-sanctions-in-relation-to-russia
- www.att.org.uk/new-financial-sanctions-relation-russia

Indicators

The UK government is targeting corrupt elites and enablers involved with assisting DPs in evading sanctions. Enablers may become a target of sanction designations themselves where they can be demonstrated to be acting on behalf of, or at the direction of, a DP, such as in the obfuscation of assets. The following indicators suspected of being used to evade sanctions have been identified through CKC casework, open source or risk monitoring by private industry.

For detection of frozen asset transfers

1. DPs communicating changes to the beneficial ownership of their corporate structures such as Private Investment Companies (PICs) and Joint Stock Companies (JSC) to non-Russian or dual national family members or associates, or nominee directors/shareholders, prior to, or shortly after sanctions taking effect. These new individuals are likely to be a front, with the DP maintaining indirect control.

2. Changes to ownership of a corporate holding to reduce ownership stakes to below the 50% threshold, shortly before or after sanctions designations. Where the transaction does not appear to be at "arms-length", the DP may still be able to initiate undue influence through associates or existing corporate governance, or through a joint arrangement with an associate or another DP in the ownership chain.

3. Movement of assets previously associated with the DP, by family members or otherwise on their behalf , such as the sale of high value assets, where funds are then disbursed offshore through secrecy jurisdictions.

4. Use of trust arrangements or complex corporate structures involving offshore companies, with circumstances of transfers calling into question whether the original owner retains indirect control or otherwise could retain a benefit from the assets transferred. Complex ownership structures could include circular ownership structures, shell companies and trust structures, with varying combinations of relatives or other close business associates of DPs operating as PSC, trustee, beneficiary, settlor, protector or other connected person.

5. Ownership transfers to previously unknown individuals, where that person's economic consumption, displays of wealth or financial footprint (such as private jets, large addresses and fleets of luxury cars) does not correspond with their newly reported wealth.

6. New equity ownership secured by long dated loan to former equity owners.

7. Multiple beneficial ownership changes synchronised with new sanctions designations.

8. Clients connected with DPs seeking to move all their assets to other financial institutions and closing their accounts in the UK.

9. Russian high-net worth individuals (HNWI) who are already on international sanctions lists, but not the UK list, who anticipate that they may become a sanctions target, transferring assets to family members and/or close associates such as employees.

10. Change in address and names for Russian entities in the lead up to the Russian invasion of Ukraine.

11. Holding companies based in jurisdictions that are offshore and/or historically linked to former Soviet Union (excluding Baltics and Ukraine) jurisdictions.

12. Change of UBOs from Russian nationals to persons of other nationalities, potentially with names of Russian origin but from third-country jurisdictions (including, but not limited to, countries that offer citizenship-by-investment schemes).

13. Investor visa or golden passport holders changing ownership information or divesting investments.

14. Beneficial ownership changes to just below aggregated thresholds.

15. 'Interim dividend' payments to provide liquidity for due considerations for beneficial ownership changes.

For detection of enablers

16. Beneficial ownership changes notified to other firms in the regulated sector accompanied by opinion of client's external counsel as to new sanctions disposition, potentially accompanied by correspondence from a senior UK company representative to convey authority.

17. Trust and Company Service Providers (TCSPs) offering nominees and trustee services to DPs and close family members or business associates.

18. Pooled accounts, in which banks see only the name of the enabler and not the client, transferring funds to entities associated in open source with DPs.

19. Use of banks and financial organisations owned by close associates of DPs.

20. Numerous transfers of shares from sanctioned entities to non-sanctioned entities involving corporations incorporated by the same people and company (often with a registered office at the same physical address).

21. A large number of off-the-shelf corporations with no trading record with nominee ownership used as throughputs.

22. Extensive personal connections between a DP and a known enabler.

23. Intelligence indicating suspicious consulting invoices at exorbitant or clearly non-market rates.

24. Material indicating that an enabler's own due diligence relies on a further layer of due diligence not actually conducted by themselves or relies on an apparently trusted (but unsubstantiated) source.

25. Material on open source, such as Companies House, indicating work for multiple sanctioned entities, such as multiple directorships.

26. The appointment of a nominee director to manage the assets of the company and beneficial ownership is obscured through the use of nominee shareholders and a deed of trust between the parties, with the DP claiming to have divested the asset.

27. The use of a complex trust structure for the ownership of a luxury asset, which is overseen by a trust company and its trustees for no apparent legitimate reason.

For detection of suspicious payments

28. Holding companies based in jurisdictions that are offshore and/or historically linked to assets in the former Soviet Union.

29. Identification of transactions by holding companies linked with DPs with Swiss bank accounts and BVI / Cypriot legal persons.

30. Payments from venture capital and private equity vehicles, many located in offshore jurisdictions, Middle East, East Asia or other jurisdictions that continue to support the Russian government or expressed neutrality in international forums such as the UN.

31. Payments received by UK businesses, often in innovative areas, such as fintechs including UK-registered payments service providers (PSPs) and electronic money institutes (EMIs), owned in part by Russian nationals and/or others implicated in previous major trade-based money laundering schemes (often involving the Baltic and Nordic states).

32. Payments via a Fintech with Russian investor nexus including customer's transactions that are initiated from or sent to IP addresses that have non-trusted sources, or are located in Russia, Belarus, jurisdictions with FATF-identified AML deficiencies or comprehensively sanctioned jurisdictions.

33. Research on private equity / venture capital vehicles and some PSC/officers of UK businesses showing individuals connected to Russian industry previously subject to sectoral sanctions and on occasion PEPs.

34. Circumvention attempts through Open Account Trade-Based Money Laundering (TBML) typology, such as increases in third party open account payments.

Industry Recommendations

1. Arms-length transactions need to be documented and should not be taken at face value by firms. Firms are advised to seek guidance from OFSI if they have any doubt. This is important not only for financial institutions, but also for professional services firms, when you are assessing indirect control a DP may exert over the entity.

2. A failure to undertake appropriate due diligence, for example wilful blindness in relation to source of funds or wealth checks, should be considered a red flag for complicity and both breach and/or circumvention offences.

3. Firms should assess complex corporate structures carefully as a component of their enhanced due diligence for high-risk clients, querying the commercial justification for such structures. As a tool of foreign policy, UK sanctions have jurisdiction both over England, Wales, Scotland and Northern Ireland, as well as the Crown Dependencies and Overseas Territories (which includes the British Virgin Islands). All UK persons worldwide are required to comply owing to the extra-territorial application of the Sanctions & Money Laundering Act 2018.

4. It should be noted that issues of aggregation of ownership can be further complicated where differing approaches to aggregation of ownership are applied across EU, UK and US and more than one owner seeks to divest their shareholding. Again, firms are advised to seek guidance from OFSI if in doubt.

5. Where firms are presented with documentation that purports to present a change in ownership by a company linked to a DP, it is important not only to conduct enhanced due diligence, but to follow up with the relevant competent authority (OFSI in the UK) to understand if firms have reason to believe that ownership has not been transferred appropriately.

6. In instances where companies have provided their own legal assessments regarding the transfer of ownership, firms should also carry out their own legal assessment in order to come to their own determination.

Data Protection Act

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

Article 5(1) 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's incompatible with these purposes;
3. Adequate, relevant and limited to what's necessary in relation to the purpose 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 purpose for which the personal data are processed;
6. Processed in a manner that ensures appropriate security of the personal data.

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 **0697-NECC** within the text. 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 of Terms. 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.

Protecting this document

This document uses the United Kingdom's Government Security Classification System (GSCS) and has been graded as **OFFICIAL**. There are no specific requirements for storage and it can be considered safe for wide distribution within your organisation and for use in staff training or awareness programmes. However, unless otherwise specified, this information is not intended for general public dissemination and should not be included on public facing websites, external mailing lists, social media or other outlets routinely used by you to deliver information to the public without the prior and specific permission of the NCA Alerts team. We therefore request that you risk manage any onward dissemination in a considered way. This document should be disposed of by cross-cut shredder, pulping or incineration.

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.nca.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.