



Office of Financial
Sanctions Implementation
HM Treasury



Financial Services Threat Assessment

February 2025



Office of Financial
Sanctions Implementation
HM Treasury



© Crown copyright 2025

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

Any enquiries regarding this publication should be sent to:
ofsi@hmtreasury.gov.uk

Contents

| | |
|---|----|
| Contents | 2 |
| Introduction | 4 |
| Key Judgements | 6 |
| Threat Overview | 7 |
| Strengthening Compliance | 9 |
| Russian Designated Persons and Enablers | 11 |
| Intermediary Countries | 24 |
| Further Resources | 27 |





The UK sanctions landscape has changed significantly since the illegal Russian invasion of Ukraine in February 2022 and the subsequent implementation of unprecedented financial sanctions on Russia by the UK Government and international partners.

Introduction

This publication is one in a series of sector-specific assessments by the Office of Financial Sanctions Implementation (OFSI) addressing threats to UK financial sanctions compliance.¹ The UK sanctions landscape has changed significantly since the illegal Russian invasion of Ukraine in February 2022 and the subsequent implementation of unprecedented financial sanctions on Russia by the UK Government and international partners. OFSI recognises the evolving nature of financial sanctions and will publish a series of assessments to assist UK firms in better understanding and protecting against threats to compliance. These assessments also demonstrate OFSI's commitment to proactively investigate breaches of UK financial sanctions.²

This assessment provides information on suspected sanctions breaches only and is intended to assist stakeholders with prioritisation as part of a risk-based approach to compliance. In some cases, including in the absence of a relevant OFSI licence, the activity described in this assessment would breach UK financial sanctions. This assessment is not necessarily a direct reflection of ongoing OFSI investigations or enforcement activity and is based on a wide range of information available to OFSI. Any references to names of individuals, entities or specific case studies in this assessment are fictional.

OFSI assesses the seriousness of suspected breaches on their merits and determines what enforcement action is appropriate and proportionate on a case-by-case basis. Guidance on breaches of financial sanctions prohibitions and OFSI enforcement can be found [here](#).

UK financial services firms

This report outlines OFSI's assessment of threats to sanctions compliance involving UK financial services firms since February 2022.³ UK financial sanctions legislation applies to all persons in the UK and UK persons wherever they are in the world. Relevant firms, as defined in legislation, comprise most of the UK financial services sector (further information on relevant firms can be found [here](#)). This includes, but is not limited to: UK financial institutions, including credit institutions; insurers; currency exchange offices; and providers of related professional services, such as accountancy service providers or auditors.⁴

The complex nature of UK financial sanctions means that most suspected breaches involve UK financial services firms in some capacity. This assessment focuses in particular on threats to compliance relating to transactions handled by UK financial or credit institutions, including banks (both retail and wholesale, which are referred to hereon as UK banks) and non-bank payment service providers (NBPSPs). For the purposes of this assessment, so-called neo or challenger banks are referred to as NBPSPs.

Since February 2022, UK financial services firms have reported over 65% of all the suspected breaches received by OFSI. Of these suspected breaches, UK banks and NBPSPs reported over 80%.⁵ This places these firms at the forefront of efforts to ensure compliance with UK financial sanctions. However, the sanctions threats outlined in this assessment are relevant to other UK financial services firms of all sizes.

Reporting to OFSI

Further information about reporting to OFSI can be found [here](#). OFSI encourages firms to report if they suspect a breach linked to the content of this assessment has occurred. Where relevant and proportionate, OFSI encourages UK financial services firms to conduct lookback exercises to identify any past suspected breaches which might not have been reported to OFSI. It will assist OFSI if firms reference “OFSI – Financial Services Threat Assessment – 0125” in any report.

Suspicious Activity Reports (SARs)

If you know or suspect that there has been money laundering or terrorist financing activity and your business falls within the regulated sector, then you are reminded of the obligations to make reports to the National Crime Agency (NCA) under Part 7 of the 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. It will help analysis if the reference “OFSI – Financial Services Threat Assessment – 0225” is included. Guidance on SARs is available [here](#).

¹ This assessment covers UK financial sanctions only and does not cover UK trade sanctions, including the Russian Oil Price Cap.

² OFSI works closely with the National Crime Agency (NCA), which is responsible for investigating suspected criminal breaches of UK financial sanctions.

³ The content of this assessment is based on information reviewed by OFSI from between January 2022 and March 2024.

⁴ This assessment does not cover cryptoasset firms, including cryptoasset exchanges.

⁵ These figures are approximate and based on suspected breaches received by OFSI from between January 2022 and March 2024.

Key Judgements

This assessment concerns sanctions threats relevant to UK financial services firms from February 2022 to present.

1. It is **likely** that some UK financial services firms, including non-bank payment service providers (NBSPs), have not self-disclosed all suspected breaches to OFSI. The timely identification and reporting of suspected breaches varies across the sector and across different UK sanctions regimes.

2. It is **highly likely** that most non-compliance by UK financial services firms has occurred due to several common issues, including the improper maintenance of frozen assets and licence conditions breaches. These issues are relevant to compliance with all UK sanctions regimes.

3. It is **almost certain** that Russian designated persons (DPs) have turned to new professional and non-professional enablers in their attempts to breach UK financial sanctions prohibitions. OFSI has observed significantly increased enabler activity since 2023.

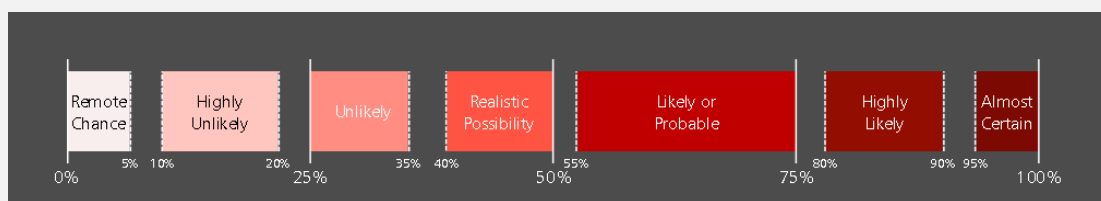
4. It is **highly likely** that enablers have made payments through NBSPs relating to the maintenance of Russian DPs' lifestyles and assets, including superyachts and UK residential properties.

5. It is **likely** a small number of enablers have attempted to front for Russian DPs and claim ownership of frozen assets.

6. Enablers have **almost certainly** used alternative payment methods, in particular cryptoassets, to breach UK financial sanctions prohibitions on Russia.

Probability Yardstick

This advisory uses probabilistic language as detailed in the Probability Yardstick developed by HMG's Professional Head of Intelligence Assessment.

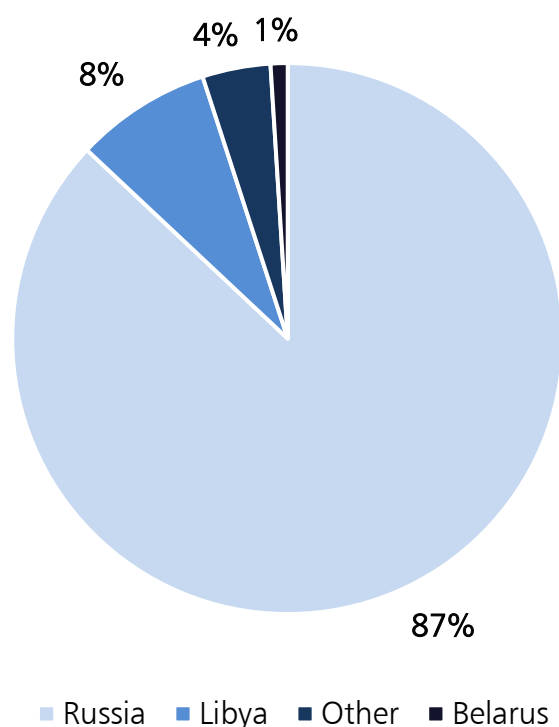


Threat Overview

A breakdown of suspected breaches reported to OFSI by UK financial services firms since February 2022 is provided below.⁶

Suspected breach reporting by regime

Over 75% of sanctions designations made by the UK Government since February 2022 have been Russia related. As shown in the graph below, Russia has also dominated suspected breaches received by OFSI from UK financial services firms since then.⁷ Although Russia sanctions remain a priority, OFSI encourages UK financial services firms to ensure robust compliance with all UK sanctions regimes. Other regimes where OFSI has identified recent threats to compliance include those relating to Libya; Belarus; Iran; and the Democratic People's Republic of Korea (DPRK).



⁶ This data is based on suspected breaches reported to OFSI between January 2022 and March 2024.

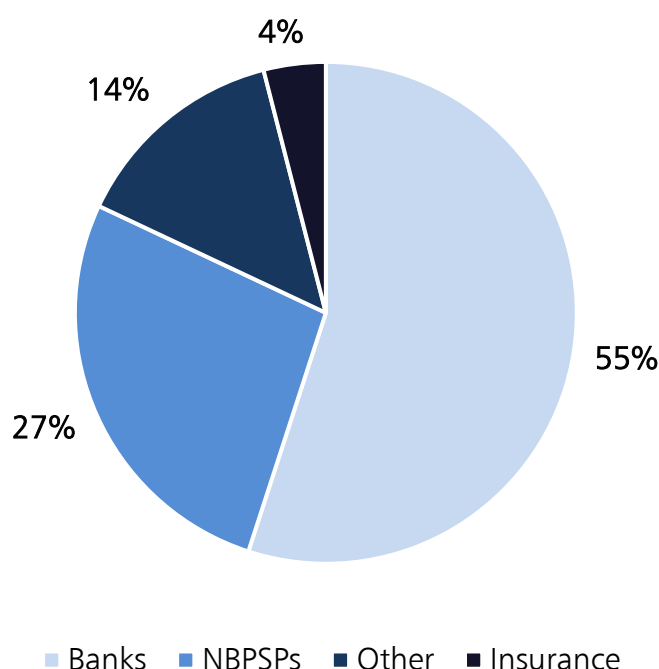
⁷ The graph on this page provides a breakdown of suspected breaches reported to OFSI by UK financial services firms by sanctions regime. The 'Other' category is an aggregation of other UK sanctions regimes which individually account for less than 1% of suspected breaches received by OFSI. These figures are approximate and based on suspected breaches reported to OFSI from between January 2022 and March 2024.

Suspected breach reporting by type of UK financial services firm

1. It is **likely** that some UK financial services firms, including NBPSPs, have not self-disclosed all suspected breaches to OFSI. The timely identification and reporting of suspected breaches varies across the sector and across different UK sanctions regimes.⁸

OFSI closely monitors suspected breaches on a sector basis to identify patterns of non-compliance. While reporting to OFSI by UK financial services firms is typically timely, OFSI has identified some substantial delays both in identifying and reporting suspected breaches. The graph below provides a breakdown of suspected breaches reported to OFSI by type of UK financial services firm.⁹

OFSI values self-disclosure of suspected breaches (further information on this can be found [here](#)). While most suspected breaches reported to OFSI from UK financial services firms are self-disclosed, OFSI has observed suspected breaches which do not lead to reports from all firms involved. OFSI also proactively investigates suspected breaches which are not self-disclosed using a wide range of available information.



⁸ When self-disclosing a suspected breach, UK financial services firms should report to OFSI and through other channels where relevant, including through SARs and to the Financial Conduct Authority (FCA). Firms should refer to OFSI guidance when self-disclosing a suspected breach.

⁹ The graph on this page provides an overview of suspected breaches received by OFSI by type of UK financial services firm. The "Other" category refers to various firms including but not limited to accountancy service providers and auditors. Insurance refers to suspected breaches unrelated to maritime transportation of certain oil and oil products and the Russian Oil Price Cap, which is not covered in this assessment. These figures are approximate and based on suspected breaches reported to OFSI from between January 2022 and March 2024.

Strengthening compliance

2. It is **highly likely** that most non-compliance by UK financial services firms has occurred due to several common issues, including the improper maintenance of frozen assets and licence conditions breaches. These issues are relevant to compliance with all UK sanctions regimes.

OFSI has reviewed a wide range of information, including suspected breaches, to identify sanctions threats and understand how compliance by UK financial services firms could be strengthened. In addition to the specific threats outlined in this assessment, this assessment highlights common compliance issues, including:

- **Improper maintenance of frozen assets.** OFSI has identified debits being made both deliberately and inadvertently from accounts held by Russian DPs at UK banks and NBPSPs. Often these transactions stem from existing insurance policies or other contracts, particularly those relating to UK residential properties. Without the correct oversight, these contracts can automatically renew and lead to debits from accounts held by DPs. Firms must ensure that all accounts and associated cards held by DPs, including those held by entities owned or controlled by DPs, are handled in accordance with asset freeze prohibitions and relevant OFSI licence permissions.
- **Breaches of specific and general OFSI licence conditions** (further information on OFSI licensing can be found [here](#)). This falls largely into three categories: transactions occurring after licence expiry, bank accounts being used other than those specified in specific OFSI licences and failures to adhere to licence reporting requirements. OFSI encourages UK financial services firms to carefully review permissions when facilitating transactions which they believe are permissible under OFSI licences. OFSI proactively monitors licence reporting and other information to ensure compliance with OFSI licence permissions.
- **Inaccurate ownership assessments.** OFSI has observed failures to identify entities which fall under the direct ownership of Russian DPs. In particular, OFSI has observed failures to identify subsidiaries owned by Russian conglomerates which are either designated themselves or majority owned by an individual Russian DP. Firms should also be alert to Russian DPs, including Russian banks, establishing new subsidiaries in intermediary countries. To mitigate the risk of inaccurate ownership assessments, firms should ensure due diligence software is updated regularly and that increased due diligence is conducted when red flags are identified.

- **Inaccurate UK nexus assessments.** A breach does not have to occur within UK borders for OFSI's authority to be engaged. There simply has to be a connection to the UK, which OFSI calls a UK nexus (further information on this can be found [here](#)). OFSI has observed across different types of transactions, particularly those involving multiple jurisdictions, failures to identify the involvement of UK nationals or entities in transaction chains. Relatedly, OFSI has also observed in some cases the incorrect identification of differences between UK, EU and US sanctions on Russia. Inaccurate assessments of how UK sanctions are engaged can result in suspicious transactions not being properly scrutinised.
- In addition to the issues highlighted above, OFSI encourages UK firms involved in correspondent banking to remain alert to non-compliance with Regulation 17A of the Russia (Sanctions) (EU Exit) Regulations 2019, which was amended with effect from December 2023 (further information on this is available [here](#)). Related to correspondent banking, OFSI encourages UK financial services firms to consider exposure to institutions who have joined the System for Transfer of Financial Messages (SPFS). Designed by the Central Bank of Russia as an alternative to SWIFT, SPFS could be used to breach UK financial sanctions prohibitions. OFSI encourages UK banks to assess their exposure to banks that have joined SPFS and to report any related suspected sanctions breaches.

Russian designated persons and enablers

3. It is **almost certain** that Russian DPs have turned to new professional and non-professional enablers in their attempts to breach UK financial sanctions prohibitions. OFSI has observed significantly increased enabler activity since 2023.

Enablers, which are defined below, can provide various services to Russian DPs, although the enabler activity which OFSI has observed falls generally into three categories:

- Making payments to maintain DPs' lifestyles and assets;
- Fronting on behalf of DPs to claim ownership or control of frozen assets and;
- Other money laundering to provide DPs with liquidity, including by using alternative payment methods such as cryptoassets.

Most Russian DPs with a historical UK nexus have left the UK since February 2022. UK financial services firms have also significantly reduced their exposure to Russia more broadly. Despite this, firms should remain alert to the threat posed by Russian DPs as well as the increasingly sophisticated methods employed by DPs and their enablers to breach UK financial sanctions prohibitions. UK banks and NBPSs in particular are well placed to identify and report enabler activity which could represent a sanctions breach.¹²

Enablers

OFSI defines enabler as any individual or entity providing services or assistance on behalf of or for the benefit of DPs to breach UK financial sanctions prohibitions. Enabler activity is any activity undertaken by these individuals or entities on behalf of or for the benefit of DPs. For the purposes of this assessment, enablers' level of complicity with sanctions breaches has been differentiated at three levels: complicit, willfully blind and unwittingly involved.¹¹

A professional enabler is defined as "an individual or organisation that is providing professional services that enable criminality. Their behaviour is deliberate, reckless, improper, dishonest and/or negligent through a failure to meet their professional and regulatory obligations".¹⁰ Professional enabler activity in the financial services sector has traditionally been associated with wealth management and other kinds of financial advisory services, particularly those based in intermediary jurisdictions offering greater secrecy through their financial and legal systems. While enabler activity of this kind has continued since 2022, as outlined below, OFSI has recently observed increased activity by new groups of professional enablers.

OFSI has also observed increased activity by non-professional enablers linked to Russian DPs. For the purposes of this assessment, such enablers are defined as individuals with close personal ties to DPs, such as their family members, ex-spouses, associates, or other proxies. While they share the same aims as professional enablers, these enablers often employ less sophisticated methods to breach UK financial sanctions.

More information on these enablers, including case studies, is provided on pages 13-22.

¹⁰ For further information, see [Red Alert](#) on Financial Sanctions Evasion Typologies By Russian Elites and Enablers, published by OFSI and the NCA in July 2022.

¹¹ NCA, National Economic Crime Centre (NECC), [Cross-System Strategy on Professional Enablers](#).

¹² The enabler activity described in this assessment refers to suspected breaches of UK financial sanctions only.

Maintaining lifestyles and assets

4. It is **highly likely** that enablers have made payments through NBPSPs relating to the maintenance of Russian DP's lifestyles and assets, including superyachts and UK residential properties.

Since February 2022, most enabler activity observed by OFSI has been linked to Russian DP's lifestyles and assets. Facing liquidity pressures due to UK financial sanctions, Russian DPs have relied on both professional and non-professional enablers to make payments to maintain their lifestyles and assets. Such payments could include those relating to: superyachts; concierge and personal security services; other property management services; school fees; and high-value goods. Without a relevant OFSI licence, these payments could breach UK financial sanctions.

Professional enablers engaging in this kind of activity are typically small companies providing services related to ultra-high-net-worth lifestyles and whose relationship with a DP likely predates designation. Non-professional enablers are typically family members, particularly children, spouses, ex-spouses and in-laws, but can also include associates.

UK financial services firms are well placed to identify enablers making payments to maintain DPs lifestyles and assets. Enabler activity of this kind often involves leveraging multiple methods of payment, including cash and cryptoassets, as well as traditional banking payments. OFSI encourages firms to remain alert to the following related red flags:

Red flags



A new individual or entity making payments to meet an obligation previously met by a Russian DP



Individuals associated with Russian DPs, including family members and professional enablers, receiving funds of significant value without adequate explanation



Frequent payments between companies owned or controlled by a DP



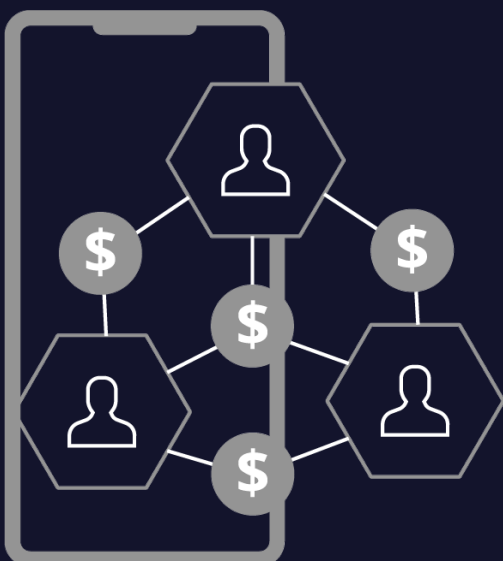
Attempts to deposit large sums of cash without adequate explanation



Cryptoasset to fiat transactions (or vice versa) involving a Russian DP's family members or associates



A family member of a DP is an additional cardholder on a purchasing card and regularly uses the card for personal expenses and overseas travel



Superyachts

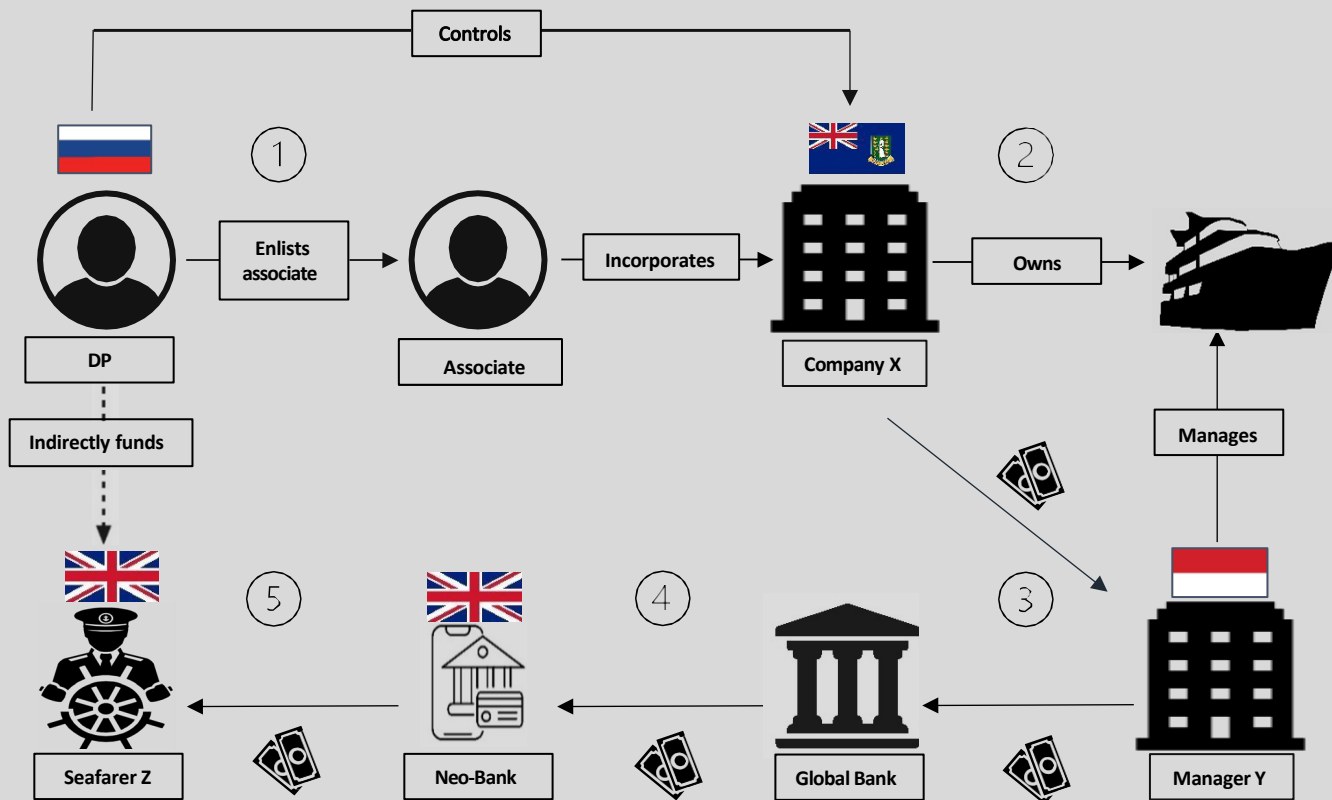
Suspected breaches under the Russia sanctions regime relating to superyachts have been persistently reported to OFSI since February 2022. Superyachts believed to be owned or controlled by Russian DPs are currently situated in various locations globally. In some cases, these superyachts are frozen due to UK, EU and US sanctions. Despite this, OFSI has identified payments being made through the UK financial services sector to staff on superyachts linked to Russian DPs following their designation. It is likely that these payments are for the continued crewing and maintenance of superyachts. In some cases, where there is a UK nexus and no OFSI licence applies, this could breach UK financial sanctions.

When reviewing related suspected breaches, OFSI has observed the persistent use of UK NBPSPs to make multiple payments internationally. UK banks, insurance providers and other UK financial services firms have also submitted reports to OFSI detailing superyacht-related suspected breaches since February 2022.

Professional and non-professional enablers have made payments relating to Russian DPs' superyachts. However, due to superyachts' specific crewing and maintenance requirements, this activity is more often associated with professional enablers. OFSI also notes that high value assets such as superyachts are often owned through opaque ownership and control structures. The case study below demonstrates how Russian DPs could leverage these structures and, with the help of professional and non-professional enablers, make payments relating to a superyacht.

UK financial services firms should report to OFSI if they identify any suspicious payments relating to Russian DPs and superyachts, including those which are owned through complex corporate structures.

CASE STUDY 1: Russian DPs with a UK nexus maintaining lifestyles and assets: superyachts



As a relevant firm, Neo-Bank fails to meet its reporting obligations if it identifies a payment from an entity it knows, or has reasonable cause to suspect, is owned or controlled by a DP.

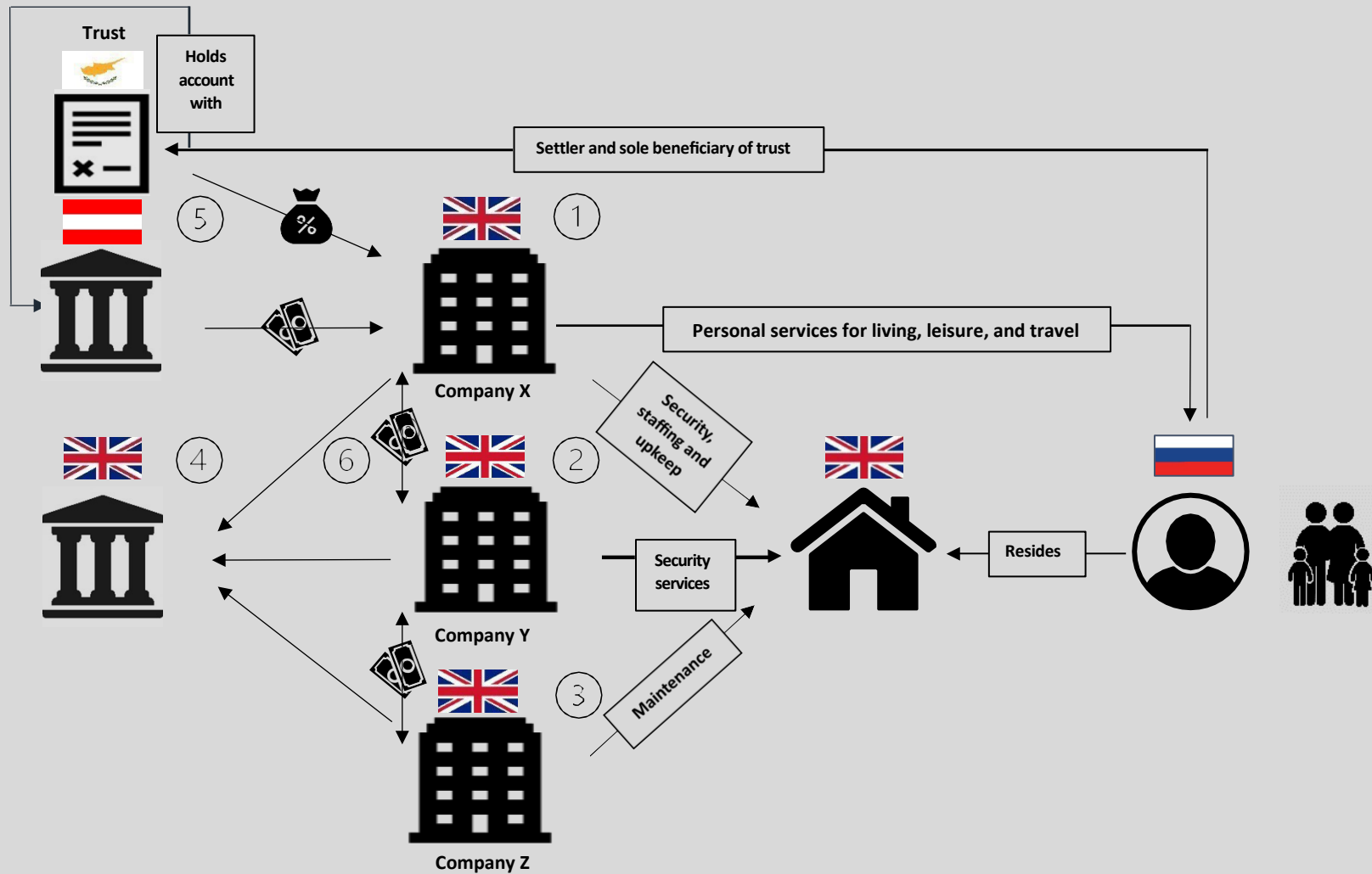
- ① A Russian DP sets up a company (Company X) in the British Virgin Islands (BVI) with the help of a non-professional enabler (Associate). Although Associate is the nominee owner of Company X, the DP holds ultimate beneficial ownership and control of Company X.
- ② Company X owns Superyacht A, which is managed by the Monaco-based Manager Y.
- ③ Manager Y banks with (non-UK) Global Bank.
- ④ On behalf of Manager Y, Global Bank remits regular salary payments to Seafarer Z, who is employed by Manager Y and works onboard Yacht A. Seafarer Z banks with UK Neo-Bank.
- ⑤ Neo-Bank fails to detect that the regular deposits it receives from Global Bank into the account of Seafarer Z are made by Manager Y, which is funded by Company X, and therefore indirectly by the DP. Since there is information in the public domain indicating that Yacht A was owned by the DP through Company X pre-designation, and Associate was a known associate of the DP, the transaction should have been subject to additional scrutiny.

UK Residential Properties

Since February 2022, OFSI has also received a significant number of suspected breach reports relating to UK residential property. Most of these suspected breaches were linked to a small number of Russian DPs with a historical UK nexus. Activities relating to UK property include but are not limited to the provision of property maintenance services; the provision of concierge or security services; property letting services; and the collection of rent from a frozen property asset, all without or outside the scope of an OFSI licence.

As with superyachts, both professional and non-professional enablers could make payments to maintain property assets owned by a Russian DP. However, OFSI has observed more professional enabler activity in this area. The case study below describes a scenario in which a professional enabler involved in property management breaches UK financial sanctions for the benefit of a Russian DP. UK financial services firms should remain alert to suspicious activity of this kind and report to OFSI where relevant.

CASE STUDY 2: Russian DPs with a UK nexus maintaining lifestyles and assets: UK residential properties



CASE STUDY 2: Russian DPs with a UK nexus maintaining lifestyles and assets: UK residential properties

- ① **Company X** is a UK registered company which provides estate management services for a Russian DP's private residence in the UK ("the Property"), including security, staffing and general upkeep of the Property and its grounds. It also provides personal services directly to the DP and their family, related to family living, leisure expenses and travel costs. **Company X** is located at the Property.
- ② **Company Y** is also a UK registered company incorporated and located at the same Property. It provides private security services to the DP.
- ③ **Company Z** is a UK registered company which provides maintenance assistance (such as electricians, plumbers and gardeners) to the Property.
- ④ All three companies are owned by a non-designated UK individual and bank with a large UK retail bank.
- ⑤ **Company X** regularly receives high value payments from accounts belonging to the DP held with an Austrian bank, as well as direct and indirect transfers from a Republic Of Cyprus-based trust, of which the DP is the settlor and sole beneficiary.
- ⑥ Funds are regularly transferred between **Companies X, Y and Z** as working capital loans or reimbursement of expenditure, indicating that the three companies share their source of wealth. The DP is the sole and/or majority client of all three companies.

All three companies are ultimately funded by the DP, provide services for the sole benefit of the DP and their family at the direction of the DP. It is therefore reasonable to expect that all three companies are controlled by the DP and are therefore also subject to UK sanctions under the Russian (Sanctions) (EU Exit) Regulations 2019.

Fronting

5. It is likely a small number of enablers have attempted to front for Russian DPs and claim ownership of frozen assets.

Since 2022, frozen assets of significant value belonging to Russian DPs have been frozen in the UK.¹³ In response to this, OFSI has identified professional enablers attempting to front on behalf of Russian DPs and claim ownership of frozen assets. Enablers of this kind could present themselves in various settings. OFSI has observed this particularly where the ownership or control of frozen assets by a Russian DP is unclear, including as a result of insolvency, complex corporate structures, and where significant liquidity is involved. In these scenarios, an enabler presenting themselves as a legitimate businessperson unconnected to a Russian DP could come forward and claim to be the owner of frozen assets. A case study based on this scenario is provided on the next page.

Enablers fronting on behalf of Russian DPs are likely to have established links to Russian DPs or Russia more broadly which they might seek to conceal. Such links are not always obvious and could include, for example, previously working for an organisation in Russia linked to a Russian DP or coming from the same community as a Russian DP. OFSI encourages UK financial services firms to take note of the following red flags, which should trigger increased due diligence:

Red flags



Individuals with limited profiles in the public domain, including those with little relevant professional experience



Inconsistencies in name spellings or transliterations, particularly those stemming from Cyrillic spellings



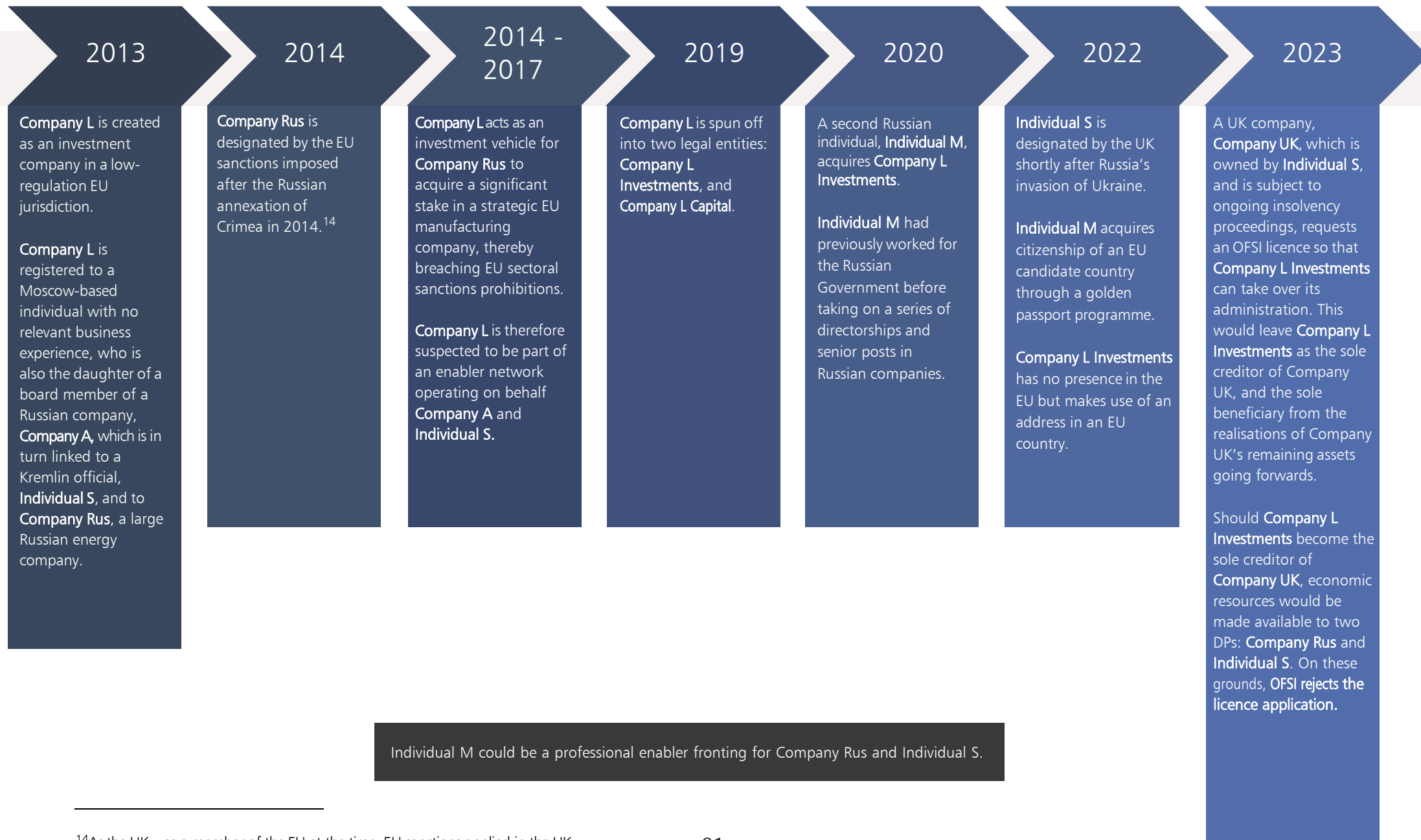
Recently acquired non-Russian citizenships, including from countries which offer golden visa schemes



Frequent or unexplained changes of name or declared location of operation

¹³The term frozen assets refers to all funds and economic resources subject to freezing under UK financial sanctions.

CASE STUDY: Professional Enablers Fronting for Russian DPs



¹⁴As the UK was a member of the EU at the time, EU sanctions applied in the UK.

Other money laundering

6. Enablers have **almost certainly** used alternative payment methods, in particular cryptoassets, to breach UK financial sanctions prohibitions on Russia.

Professional enablers forming part of established criminal networks have also been linked to Russian financial sanctions breaches. In December 2024, an NCA-led investigation exposed and disrupted a Russian money laundering network employing complex methods to breach financial sanctions implemented by the UK Government and international partners.¹⁵

Operating internationally, this group provided a variety of services, including a system for exchange of cash to crypto (and vice versa) and the laundering of funds linked to property purchases in the UK. Cryptoassets and cash couriers played a central role in these activities. As noted by the NCA, the Russian money laundering group had significant exposure to the UK-designated cryptocurrency exchange Garantex. The group also extensively exploited dollar-backed stablecoins such as Tether (USDT).

Although often difficult to detect, OFSI encourages UK financial services firms to remain alert to attempts at money laundering by or on behalf of Russian DPs, including any indications of high value cryptoasset to cash (or vice versa) transfers.

¹⁵ NCA Operation Destabilise [press release](#), published 4th December 2024



Since February 2022, over 25% of suspected breach reports received by OFSI from UK financial services firms have made reference to intermediary jurisdictions.

Intermediary countries

Suspected breaches of UK financial sanctions prohibitions by Russian DPs often involve intermediary jurisdictions. Individual Russian DPs have traditionally structured their interests, including the ownership and control of assets, through a small number of favoured intermediary jurisdictions. While some intermediary jurisdictions offer greater secrecy through legal and financial systems, intermediary jurisdictions that do not offer secrecy have historically also been attractive to Russian investors for commercial reasons due to the services and products that they offer, and/or their links to major markets.

Reflecting this, since February 2022, just over 25% of suspected breach reports received by OFSI from UK financial services firms have made reference to intermediary jurisdictions. The following jurisdictions feature most often: British Virgin Islands (BVI); the Republic of Cyprus; Switzerland; United Arab Emirates (UAE); Guernsey; Luxembourg; Austria; and Türkiye.¹⁶

OFSI has also observed a shift in the third countries referenced in suspected breach reports over time. In 2022, the countries referenced most often in suspected breaches reported to OFSI were the BVI, Switzerland, and the Republic of Cyprus. In 2023, OFSI noted that, while links to BVI, the Republic of Cyprus, and Switzerland remained prevalent, there was an increase in reports involving the Isle of Man, Türkiye, the UAE, and Guernsey. In the first quarter of 2024, cases referencing the UAE made up the largest section of suspected breaches reported to OFSI, followed by Luxembourg, the Cayman Islands and the Republic of Cyprus.

The change in the countries referenced in OFSI suspected breach reports has likely been driven by several factors, including Russian capital flight to jurisdictions which do not have sanctions on Russia, such as the UAE and Türkiye.

Throughout its analysis of suspected breach reports, OFSI has observed increased instances of specific activities in certain countries, which could be indicative of UK financial sanctions breaches. While the activities described below do not always signify suspected breaches in and of themselves, they are linked with illicit sanctions activity in that jurisdiction and should therefore trigger increased due diligence. These activities are particularly relevant to financial services firms operating in or transacting with firms in these countries.

¹⁶ It should be noted that a reference to an intermediary jurisdiction in a report of a suspected sanctions breach does not necessarily mean that any sanctions breach has occurred in that jurisdiction, or that the jurisdiction does not enforce sanctions effectively.

| Country | Activity |
|------------------------|--|
| Austria | <ul style="list-style-type: none"> • Enabler activity • Non-resident banking¹⁷ • Transactions involving cryptoassets |
| BVI | <ul style="list-style-type: none"> • Ownership or transfers of assets • Money laundering networks • Use of complex corporate structures such as trust arrangements or complex corporate structures involving offshore companies |
| Switzerland | <ul style="list-style-type: none"> • Networks used to process the funds of UK sanctioned individuals • Non-resident banking |
| The Republic of Cyprus | <ul style="list-style-type: none"> • Ownership or transfers of assets • Enabler activity • Use of complex corporate structures such as trust arrangements or complex corporate structures involving offshore companies |
| UAE | <ul style="list-style-type: none"> • Ownership or transfers of assets • Enabler activity • Networks used to process the funds of UK sanctioned individuals • The setting up of new companies which appear to be copies of the companies that have been closed down in other jurisdictions • Transactions involving cryptoassets |

| | |
|---------|---|
| Türkiye | <ul style="list-style-type: none"> • Enabler activity • Maintenance and crewing of superyachts owned or controlled by Russian DPs • Non-resident banking |
|---------|---|

| | |
|----------------|---|
| Cayman Islands | <ul style="list-style-type: none"> • Offshore account payments • Enabler activity |
|----------------|---|

OFSI is providing this information to UK financial services firms to inform a risk-based approach to compliance. Firms should consider the involvement of intermediary jurisdictions alongside other red flags of sanctions breaches, including those detailed in this assessment, and report to OFSI where relevant.

¹⁷For the purposes of this assessment, non-resident banking refers to banking services provided to individuals or entities that do not reside in the jurisdiction where the bank is located.

Further resources

This assessment highlights OFSI's ongoing commitment to proactively engage with stakeholders to ensure UK financial sanctions are properly understood, implemented and enforced in the UK. OFSI will publish further sector-specific assessments in 2025 which are also likely to be relevant to UK financial services firms. OFSI has also published, and will continue to do so, information on specific threats to UK financial sanctions compliance, including, for example, the recent advisory on North Korean IT workers (available [here](#)).

This assessment does not represent legal advice and should be read in conjunction with OFSI guidance (available [here](#)). OFSI also encourages firms to review Frequently Asked Questions (FAQs) published by OFSI which provide short form guidance and technical information on financial sanctions (available [here](#)).

This assessment builds on previous and related publications issued by OFSI and UK Government partners, including the [Red Alert](#) on Financial Sanctions Evasion Typologies By Russian Elites and Enablers, published by OFSI and the NCA in July 2022. OFSI encourages UK financial services firms to review publications from other relevant UK Government bodies, including the NCA and the Financial Conduct Authority (FCA).



Office of Financial
Sanctions Implementation
HM Treasury