

Global Advisory on Russian Sanctions Evasion

Issued Jointly by the Multilateral REPO Task Force

March 9, 2023

Overview

Shortly following Russia's invasion of Ukraine in February 2022, Australia, Canada, France, Germany, Italy, Japan, the United Kingdom, the United States, and the European Commission launched the Russian Elites, Proxies, and Oligarchs (REPO) Task Force, a multilateral effort that has used information sharing and coordination to isolate and exert unprecedented pressure on sanctioned Russian individuals and entities. The REPO Task Force, consisting of Finance Ministry and Justice or Home Ministry participation in each member jurisdiction, has successfully used their respective authorities to track Russian sanctioned assets and heavily restrict sanctioned individuals and entities from accessing the international financial system. The REPO Task Force's work has leveraged cooperation from like-minded countries outside of the task force and worked in close coordination with the European Commission's Freeze and Seize Task Force. These efforts have denied regime insiders access to revenue streams and economic resources used to support Russia's war of aggression in Ukraine.

The REPO Task Force's collective efforts have resulted in the freezing of tens of billions of dollars and the freezing or seizure of high-value goods or property. However, some sanctioned Russian elites and their financial networks have managed to evade sanctions and, in some instances, maintain access to funds. Additionally, in some instances, sanctioned individuals and entities may be able to generate additional revenue or procure export-controlled and sanctioned items. This illicit financial activity runs in direct contravention of the multilateral sanctions that impose costs on Russia for its unprovoked war and deny the access of sanctioned Russian individuals and entities to the international financial system.

To underscore the REPO Task Force's commitment to work collaboratively with the private sector, and to deny key Russian elites and proxies' access to revenue and sensitive goods and technologies, the REPO Task Force has identified certain typologies of Russian sanctions evasion tactics and is issuing recommendations to mitigate the risk of exposure to continued evasion. This advisory will contribute to effective sanctions implementation across REPO Task Force members' jurisdictions by preventing the undermining of financial sanctions, export controls, and other restrictive measures designed and implemented in response to Russia's unprovoked war of aggression in Ukraine. Typologies identified in this advisory include: the use of family members and close associates to ensure continued access and control; the use of real estate to hold value, benefit from wealth; the use of complex ownership structures to avoid identification; the use of enablers to avoid involvement, leverage expertise; and the use of third-party jurisdictions, false trade information to facilitate sensitive goods shipment to Russia.

To complement this effort, private sector partners should closely review advisories and publications issued by REPO Task Force members relevant to the jurisdictions and industries in which they operate. The REPO Task Force remains committed to continued collaboration and coordination to restrict sanctioned individuals and entities from using the international financial system to fund Russia's brutal war of aggression and to ensuring effective and robust enforcement of sanctions, including by criminal prosecution.

Typologies of Russian Sanctions Evasion

Use of Family Members and Close Associates to Ensure Continued Access and Control

REPO Task Force members identified various instances in which Russian elites transferred the beneficial ownership of legal entities and arrangements and other property to their children, in an attempt to ensure continued control as well as access to wealth after the imposition of sanctions.¹ In another instance, REPO members determined that designated oligarchs directly transferred the funds to family members in an attempt to hide assets.² Family members and close associates of designated persons are well placed to act as proxies and facilitate this kind of sanctions evasion and illicit financial activity.³ Asset transfers to family members or close associates sometimes occur in the period immediately leading up to a designation or closely thereafter, which may indicate an attempt to evade sanctions on the part of the sanctioned individual and the party that facilitated the transfer.⁴ In addition to being able to exercise control through their proxies in these types of arrangements, ostensibly moving control or funds to a family member or close associate also conveniently allows the designated person to avoid scrutiny from both regulated industries and the competent authorities. Finally, depending on the facts and circumstances, there could be sanctions risk related to arrangements that attempt to hide assets, obscure sanctioned interests, or otherwise evade scrutiny, and REPO members may seek to impose sanctions on the family members and close associates seeking to facilitate these types of arrangements.

Use of Real Estate to Hold Value, Benefit from Wealth

Historically, Russian oligarchs and elites have invested in properties around the world, and it has been reported publicly how many enjoy the benefits of their real property.⁵ Since the invasion of Ukraine, however, there has been an increase in the use of real estate as a vehicle to hold Russian wealth. Some of these investments and purchases could be indicative of sanctions evasion activity.⁶

Specifically, sanctioned Russian individuals and entities may launder or attempt to launder and obfuscate illicit proceeds—including those derived from sanctions evasion—through the purchase of real estate, often hiding behind intermediaries, nominees or straw purchasers and/or opaque corporate structures including legal entities or trusts.⁷ Another sign indicative of sanctions evasion

1 See National Crime Agency, National Economic Crime Centre, Joint Money Laundering Intelligence Taskforce, and Office of Financial Sanctions Implementation, [“Financial Sanctions Evasion Typologies: Russian Elites and Enablers.”](#) (July 2022); see also Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), [“Special Bulletin on Russia-linked money laundering related to sanctions evasion.”](#) (March 2022).

2 See Financial Crimes Enforcement Network (FinCEN), [“Trends in Bank Secrecy Act Data: Financial Activity by Russian Oligarchs in 2022.”](#) (December 22, 2022).

3 See FinCEN, [“FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members.”](#) (March 16, 2022).

4 See also European Commission, [“Commission Consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014.”](#) at FAQ B.1.5 (last updated February 7, 2023).

5 See Forbes, [“A Guide To All The Outrageous Mansions and Estates Owned By Sanctioned Russian Billionaires.”](#) (March 5, 2022); see also FinCEN, [“Advisory to Financial Institutions and Real Estate Firms and Professionals.”](#) (August 22, 2017).

6 See, e.g., U.S. Department of Justice, <https://www.justice.gov/usao-sdny/pr/uk-businessman-arrested-sanctions-evasion-benefitting-russian-oligarch-oleg-deripaska> (October 11, 2022).

7 See FinCEN, [“FinCEN Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies.”](#) (January 25, 2023).

activity may follow a known money laundering typology—the purchase of real property below or above its market value—as well as the use of offshore buyers with potential links to Russia. Additionally, a sanctioned Russian or their proxy’s ability to acquire real property may help with attempts to “secure residency and/or citizenship,” in a country possibly perceived as having lower illicit finance risks, “...conveying social respectability, and providing an immediately available good of material benefit that may appreciate in value.”⁸

Use of Complex Ownership Structures to Avoid Identification

Money launderers and other illicit actors often use shell companies or other legal entities and arrangements to avoid detection—sanctioned Russians individuals and entities and their proxies are no different. Schemes that have been uncovered over the years by competent authorities show how these actors leverage complex ownership structures to disguise their connections to particular assets or entities.⁹ Designated persons may further obfuscate their involvement in sanctions evasion schemes and efforts to stash away their wealth by using a combination of legal entities and legal arrangements such as trusts to ensure they remain undetected.¹⁰ Specifically, REPO members have discovered trust arrangements that may have been designed to thwart sanctions enforcement. These arrangements may indicate that everyone involved in the trust—including law firms, grantors (also defined as protectors), trustees, settlors, and beneficiaries—may be involved in sanctions evasion. In some instances, sanctioned Russians individuals and entities and their proxies may involve relatives and close associates in these legal structures and arrangements to further obfuscate their ownership or relation to the assets.¹¹ It is not uncommon for these legal entities and arrangements to be located in jurisdictions that are tax or corporate formation havens, which may afford a degree of secrecy to Russian elites and their proxies.¹² Additionally, attention should be paid to transactions that involve shell companies registered in traditional tax havens conducting international wire transfers using financial institutions in jurisdictions distinct from the company’s registration (non-resident banking).¹³

Use of Enablers to Avoid Involvement, Leverage Expertise

Sanctioned Russian individuals and entities may attempt to avoid direct participation in sanctions evasion activity by utilizing certain persons in key professions, including those that frequently interact with the international financial system. These persons, known as enablers, may leverage their ability to open bank accounts, send and receive money, and create corporate structures—among other

8 See Financial Action Task Force, [“Risk Based Approach Guidance for the Real Estate Sector,”](#) (July 26, 2022); see also FINTRAC, [“Special Bulletin on Russia-linked money laundering related to sanctions evasion,”](#) (March 2022).

9 See U.S. Department of the Treasury, [“U.S. Treasury Blocks Over \\$1 Billion in Suleiman Kerimov Trust,”](#) (June 30, 2022); see also FinCEN, [“FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members,”](#) (March 16, 2022).

10 See, e.g., U.S. Department of Justice, [“Arrest and Criminal Charges Against British and Russian Businessmen for Facilitating Sanctions Evasion of Russian Oligarch’s \\$90 Million Yacht,”](#) (January 20, 2023).

11 See National Crime Agency, National Economic Crime Centre, Joint Money Laundering Intelligence Taskforce, and Office of Financial Sanctions Implementation, [“Financial Sanctions Evasion Typologies: Russian Elites and Enablers,”](#) (July 2022); see also FinCEN, [“FinCEN Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies,”](#) (January 25, 2023).

12 See, e.g., FINTRAC, [“Special Bulletin on Russia-linked money laundering related to sanctions evasion,”](#) (March 2022).

13 *Id.*

functions—to directly and indirectly aid sanctioned persons’ evasion efforts.¹⁴ The enabler will often perform certain functions on behalf of the sanctioned person to allow the sanctioned party continued access to their funds. Enablers may operate in offshore financial centers where company formation is common. Enablers can include lawyers¹⁵, accountants, as well as trust and company service providers.¹⁶ An additional type of enabler that sanctioned persons may utilize is an individual or entity that helps consolidate investments from high-net worth individual or institutional investors. These types of individuals and entities help “feed” or aggregate investments for placement into a private fund that the investors may not be able to access on their own because they do not meet asset or income requirements to invest in private funds, lack the relationship with advisers of private funds, or wish to avoid disclosing their identities.¹⁷

Use of Third-Party Jurisdictions, False Trade Information to Facilitate Sensitive Goods Shipment to Russia

The REPO Task Force members’ sanctions, export controls, and restrictive measures deprive the Russian regime of revenue and prevent access to sensitive goods—including dual use goods—to support Russia’s military industrial complex.¹⁸ However, REPO Task Force members have identified that some Russian end-users continue to seek—and, in some cases, gain—access to sensitive goods.¹⁹

One method Russian end-users use is to list a freight forwarding business, often located in third party jurisdictions, as the final destination of a good, when in fact those goods will be further shipped to their intended final destination in Russia. The entities facilitating these transactions may often appear to have no affiliation with the transaction and may be utilizing a known trans-shipment point.²⁰ These Russian end-users may rely on false documentation, to include bill of lading information and other supporting documentation such as fraudulent trade finance information, to ensure the delivery of goods.²¹

14 On May 8, 2022, in consultation with the U.S. Department of State, the Office of Foreign Assets Control (OFAC) issued a determination that prohibits the exportation by U.S. persons of certain services, including trust and corporate formation services, to any person located in the Russian Federation. See U.S. Department of the Treasury, [“Determination Pursuant to Section 1\(a\)\(ii\) of Executive Order 14071.”](#) (May 8, 2022).

15 In some instances, certain legal services to sanctioned persons may be permissible, for example, OFAC has issued certain general licenses authorizing the provision of certain legal services, see Russian Harmful Sanctions Regulations, 31 C.F.R. Part 587, [“§ 587.506 Provision of certain legal services;”](#) see also Russian Harmful Sanctions Regulations, 31 C.F.R. Part 587, [“§ 587.507 Payment for legal services from funds originating outside the United States.”](#)

16 See National Crime Agency, National Economic Crime Center, Joint Money Laundering Intelligence Taskforce, and Office of Financial Sanctions Implementation, [“Financial Sanctions Evasion Typologies: Russian Elites and Enablers.”](#) (July 2022).

17 See U.S. Department of the Treasury, [“Remarks by Assistant Secretary for Terrorist Financing and Financial Crimes Elizabeth Rosenberg ABA-ABA Financial Crimes Enforcement Conference.”](#) (December 05, 2022).

18 For a list of “commodities of concern,” see FinCEN, [“FinCEN and the U.S. Department of Commerce’s Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts.”](#) (June 28, 2022).

19 See U.S. Department of the Treasury, [“Treasury-Commerce-State Alert: Impact of Sanctions and Export Controls on Russia’s Military Industrial Complex.”](#) (October 14, 2022); see also U.S. Department of the Treasury, [“Treasury Sanctions Global Russian Military Supply Chain, Kremlin-linked Networks, and Elites with Western Fortunes.”](#) (November 14, 2022).

20 See FinCEN, [“FinCEN and the U.S. Department of Commerce’s Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts.”](#) (June 28, 2022).

21 See also European Commission, [“Commission Consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014.”](#) at FAQs A.2, D.2 (last updated February 7, 2023).

Ongoing International Cooperation on Russia-Related Illicit Finance Issues

Members of the Russia-Related Illicit Finance and Sanctions (RRIFS) international working group of Financial Intelligence Units have observed similar trends/typologies in relation to the associated illicit activities of the unjustified invasion of Ukraine by the Russian Federation including money laundering, sanctions evasion, cyber threats, and corruption. A specific example of these observations by a RRIFS member is provided in FinCEN's [Financial Trends Analysis-Trends in Bank Secrecy Act Data: Financial Activity by Russian Oligarchs in 2022](#), FINTRAC's [Special Bulletin on Russia-linked money laundering related to sanctions evasion](#), and FIU-Latvia's study on [Indicators of Russia-Related Sanctions Evasion](#). Since launching the working group in March 2022, RRIFS members have worked within their respective mandates and authorities to surge the sharing of tactical financial intelligence on these illicit activities and develop a common base of understanding among RRIFS members through dissemination of strategic-level intelligence on a variety of related issues (such as trends, typologies, relevant money laundering indicators, and jurisdictions of interest). RRIFS members remain committed to cooperate with law enforcement, other competent authorities, and the private sector, within the legal framework of their respective AML/CFT regimes, to achieve the goals of the international working group

Recommendations

Ensure Compliance with National Rules Incorporating FATF Recommendations

Regulated entities²², whether financial institutions or designated non-financial businesses and professions, should follow the Financial Action Task Force (FATF) recommendations as implemented by their jurisdiction. This includes designing appropriate risk mitigation measures to prevent illicit financial activity, such as the use of shell companies or nominees.

Ensure Compliance Program Implements Relevant AML/CFT Laws and Regulations and is Regularly Reviewed

Regulated entities should also take all necessary measures to comply with AML/CFT laws and regulations, and reporting requirements—to include those related to suspicious transaction reports—as set out by their jurisdictions. Regulated entities maintain an obligation to identify and report on illicit activity and their continued adherence to AML/CFT laws and regulations is integral to REPO member's efforts to counter illicit financial activity, to include Russian sanctions evasion, across jurisdictions.

Take Part in Existing Public-Private Partnerships

Regulated entities are an integral part in the joint effort among REPO Task Force members to prevent Russian sanctions evasion activity. Regulated entities' unique role in the international financial system provides them with valuable data and insight to mitigate the risk of Russian sanctions evasion activity. However, their positioning generally is limited to a private sector perspective. Regulated and non-regulated entities alike should consider taking part in existing public-private partnerships with competent authorities; these arrangements may offer an opportunity to regulated entities to hear from

²² Regulated entities are private sector entities with anti-money laundering/countering the financing of terrorism (AML/CFT) responsibilities required by law.

competent authorities and gain their perspective on Russian sanctions evasion to inform their efforts.²³ At the same time, competent authorities can learn from regulated entities to become more aware of the risks, trends, and typologies identified by the private sector. Competent authorities and private sector entities alike should explore the opportunity of further engagement in this space to counter Russian sanctions evasion efforts as well as other forms of illicit finance. Such engagement may also be valuable in promoting cooperation with competent authorities to detect, report, and address potentially violative conduct.

Leverage Information Sharing Protocols

Regulated entities' access to valuable information such as customer information, transaction details, and trade documentation, puts them on the front line in the fight against illicit finance and Russian sanctions evasion and allows them to identify suspicious activity. However, sometimes these regulated entities' positioning may only provide them with a limited view of the underlying activity of concern, focused on specific customers or business lines. To overcome this obstacle, regulated entities should utilize existing information sharing mechanisms, if feasible in their respective jurisdictions, to leverage other regulated entities' data holdings and unique positioning to enhance their efforts to identify and mitigate the risk of Russian sanctions evasion activity.

Update Risk Assessments

Regulated entities often rely on internal risk assessments to inform their efforts to mitigate illicit finance risks where applicable—including Russian sanctions evasion—that their businesses face. Since Russia's invasion of Ukraine, the global financial and trade systems have changed dramatically, as various players have sought to find new avenues to substitute now closed off routes across the world. Regulated entities should be aware of the changes in illicit behavior and how they materialize into risks that their business face. Ensuring that risk assessments remain up to date is a key way to capture these changes that threaten their businesses.

²³ FinCEN Exchange is one example of the many information-sharing authorities and programs in the United States, including private-to-private information sharing and other public-to-private information sharing authorities. FinCEN Exchange is FinCEN's voluntary public-private information sharing partnership among law enforcement, national security agencies, financial institutions, and other relevant private sector entities aimed at effectively and efficiently combating money laundering, terrorism financing, organized crime, and other financial crimes; protecting the financial system from illicit use; and promoting national security. FinCEN has hosted operationally-focused Exchanges that brought together particular law enforcement agencies and key financial institutions to assist in advancing particular investigations and priorities, such as sanctions evasion. The operationally-focused objective, in part, is to establish two-way information sharing to create an accelerated cycle of financial intelligence sharing.

Increase Awareness of Sanctions Risk and Its Impact for Non-AML/CFT Regulated Entities

Sanctions apply to all natural and legal persons under the relevant jurisdiction of the sanctions-issuing authorities. While much of the focus on entities is towards those regulated for AML/CFT, many economic operators and entities that are not regulated for AML/CFT face sanctions risk and exposure.²⁴ Economic operators and entities should seek out educational opportunities and engagements so that they may better understand sanctions and their implementation to ultimately avoid facilitating Russian sanctions evasion.²⁵ At the same time, these types of economic operators and entities should remember the importance of investing in sanctions compliance measures to operationalize their risk mitigation measures and ensure compliance with sanctions enacted in their respective jurisdictions.²⁶

24 See, e.g., Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, [“Gels des Avoir – Direction Générale du Trésor.”](#)

25 See, e.g., European Commission, [“Commission Consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014.”](#) at FAQ A.2 (last updated February 7, 2023); see also U.S. Department of the Treasury, [“A Framework for OFAC Compliance Commitments.”](#) (May 2019).

26 See, e.g., Government of Canada, [“Advisory to Canadian Businesses on Canada’s Sanctions Related to the Russian invasion of Ukraine.”](#) (September 2022).