NEW ZEALAND
FOREIGN AFFAIRS & TRADE
Manatū Aorere

RUSSIA SANCTIONS GUIDANCE
MAY 2024

Sanctions Evasion: Common Red Flags

What this guidance covers

This guidance note describes Russia sanctions red flags to look for when carrying out due diligence about your trading activities, your customer or someone else you may have dealings with.

It does not exhaustively assess every threat, vulnerability or control in relation to Russia sanctions evasion.

The guidance should be read in conjunction with the Russia Sanctions Act 2022, the Russia Sanctions Regulations 2022 and *Guidance note: Understanding evasion risks and implementing due diligence in the Russia Sanctions context*.

Notes

- This guidance does not constitute legal advice.
- It is not intended to provide guidance in relation to United Nations sanctions, or autonomous sanctions regimes of other countries relating to Russia or otherwise.
- Examples are provided to assist people in meeting their obligations under the Act and Regulations but are not intended to be definitive or exhaustive.
- This guidance will be updated over time. Please continue to check the MFAT website to ensure you are using the most recent version of this guidance.
- If you have any questions about this guidance, please contact the team at the New Zealand Sanctions Unit at sanctions@mfat.govt.nz.

Contents

Document version information

VERSION NUMBER	DESCRIPTION	DATE
1.0	First issue	XX April 2024

1. Introduction

1.1 Why do we have sanctions?

Sanctions are a tool to express New Zealand's serious condemnation of Russia's illegal invasion of Ukraine and to exert pressure on Russia to change its course of behaviour.

Sanctions operate in an international context and are most effective when they complement or reinforce sanctions taken by other countries.

New Zealand's Russia Sanctions Act 2022 (the Act) and Russia Sanctions Regulations 2022 (the Regulations) place a range of obligations on all New Zealanders by prohibiting or restricting specific activities as part of this global effort, including dealings with sanctioned persons, assets, services and securities.

You can find further explanation of the purpose of sanctions and the rules, policies, and procedures that make up the Russia sanctions regulatory system in the *Russia Sanctions Regulatory Charter*.

1.2 Protecting New Zealand persons from being used to evade sanctions

Sanctions prevent New Zealand persons from having dealings with sanctioned persons, assets and services, or with those who act on their behalf. Sanctions evasion is the act of avoiding or circumventing sanctions.

While New Zealand's exposure to sanction evasion risk may be less than others due to our distance and relatively limited trade and economic relationships with Russia, New Zealanders can still be used by others to evade sanctions of like-minded partners.

So, it is prudent to consider if there are any 'red flags' relating to your usual business that may indicate sanction evasion activity. This includes understanding and looking for the common techniques and methods of sanction evasion and their associated actions and behaviours.

You can learn more about the evasion landscape and appropriate due diligence in *Guidance note: Compliance, due diligence and understanding evasion risks in the Russia Sanctions context*.

2. What are red flags?

Appropriate due diligence will help support your compliance with the Act and the Regulations before entering into a business relationship or transaction, and will help you avoid supporting attempts at sanctions evasion. During the course of due diligence you may identify "red flags".

Red flags are types of activities that, depending on the nature and purpose of the business relationship, would raise questions about the purpose of that activity.

Knowing what red flags to look for may help you identify potential risks. For example, if a customer seeks to conduct a complex and unusually large transaction, or undertakes unusual patterns of transactions with a country bordering a conflict zone.

Each industry or sector faces their own threats and vulnerabilities and corresponding red flags. Red flags by themselves may not indicate sanction evasion activity, but would trigger the need for enhanced due diligence measures.

2.1 Trigger events can change or create new red flags

Changes in sanctions evasion tactics and red flags can be the result of 'trigger events'. For example:

- Changes in policy – Developments in the war in Ukraine could result in domestic and/or international changes in sanctions policy.
- New and emerging sanction evasion techniques – Refinements of old techniques and the emergence of new sanction breaching tactics can reduce the effectiveness of existing controls. Red flag alerts need to be tested to ensure they remain fit for purpose.
- New technology – New and developing technologies/products can present previously unknown sanction vulnerabilities and bypass existing sanctions measures in the effort to achieve anonymity and disguise beneficial ownership.
- Changes in management/decision makers – Changes to how a business is managed could lead to a re-appraisal of the appetite for risk associated with sanction evasion.

3. Common techniques, methods and red flags

Common techniques and methods used for Russia sanction evasion, along with their associated red flags, have been identified by various reviews undertaken globally. The tables and lists of red flags below draw on this work. They are not exhaustive and are provided for illustrative purposes. Links to some of the more detailed public reference sources are included in section 4 (page 11) to support your ongoing risk management work.

Guidance on evasion techniques, methods and red flags has been broken down under the following headings:

- **Import and export of goods** – this includes freight forwarding, import/export controls, and procurement networks.
- **Know your customers** – this includes complex corporate structures, beneficial ownership, and the use of real estate, professional services, relatives and close associates to obfuscate.
- **Financial systems** – this includes the financial sector, virtual assets and techniques for hiding assets.
- **Maritime transport** – this includes vessels going dark, ship-to-ship transfers and other cargo and vessel misleading information.

3.1 Import and export of goods

Common technique	Red flags
Using freight forwarders to mask beneficial ownership and ultimate destination of goods	• Transactions involving freight-forwarding firms that are also listed as the product's end customer, especially items going to traditional Russian trans-shipment hubs. • The customer or purchasing agent is reluctant to offer information about the end-use of the item. • Delivery dates are vague, or deliveries are planned for out of the way destinations. • Parties listed as consignees do not typically engage in business consistent with the products involved.
Sourcing components or sub-components from a variety of suppliers	• Accessing items from multiple sources to disguise the true nature and purpose of procurement. • Product nature and capabilities do not fit the buyer's line of business • Items ordered are incompatible with the technical level of the destination country. For example, semiconductor manufacturing equipment shipped to a country with no electronics industry. • Routine installation, training, or maintenance services are declined by the customer. • Packaging is inconsistent with the stated method of shipment or destination.
Mislabelling imports and exports	• Discrepancies between shipped goods and their declared value, quantity, or description. Inconsistencies may arise from forged or altered documents or collusion between parties to a transaction. • Deliberate misrepresentation of the value of goods. Overvaluing imports or undervaluing exports enables the transfer of excess funds to foreign suppliers or buyers. • Misleading information which obfuscates the nature of items or disguises the ultimate destination.
Using third-country transhipment locations	• Freight forwarding from transit hubs re-directs goods to sanctioned countries with or without the knowledge of the original exporter.
Financial services or transactions physically distanced from the physical trade in goods	• A New Zealand-registered company using onshore financial services to receive payment but shipping goods from an offshore operational location.
Originally bound for Russia but now diverted	• Transactions originally destined for Russia, Belarus or a company located in Russia or Belarus, but details are changed to a different country/company without trade restrictions.

3.2 Know your customer

Common technique	Red flags
Using front or shell companies	• Using front or shell companies (onshore and offshore) and professional intermediaries to mask parties to transactions and end users. • Using front or shell company/trust structures to hide and disguise beneficial ownership and effective control. • Overly complex corporate and ownership structures. • Organisational structure is confusing and deflects scrutiny. • Company/Trust registered in a country with previous history of sanctions evasion • Entities may have corporate names that are overly generic, non-descriptive, or easily mistaken with that of a better-known corporate entity. Additionally, the corporate name may be regularly misspelled in different ways. • Procurement through complicit New Zealand companies using unwitting third-party New Zealand suppliers. • Jurisdictions previously associated with Russian financial flows that are identified as having a notable recent increase in new company formations. • Holding companies based in offshore jurisdictions or regions historically linked to former Soviet Union jurisdictions (excluding Baltics and Ukraine). • A large number of off-the-shelf corporations with no trading record, with nominee ownership used as throughputs. • 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). • Shell and front companies with little to no, or suspicious, online presence. This would include companies where websites lacking normal business information such as products and services, contact details, geographic location.
Using overly complex transactions	• Convoluted financial routes to hide the final destination or the ultimate beneficiary, such as transfers to third countries not of sanction concern. • Parties to transactions with addresses that do not appear consistent with the business or are otherwise problematic (e.g., physical address does not exist, or it is a residential address).

Retaining influence through trusted proxies and enablers	• Using professional services to exert influence while hiding effective control. Relevant professions include but are not limited to: legal (barristers and solicitors); financial (relationship managers, accountants, investment advisors, wealth managers, payment processors, private equity, TCSPs); estate agents; auction houses; company directors; intermediaries/agents; and private family offices. • Use of professional services, such as trustees, nominee directors, lawyers or accountants in New Zealand, despite no legitimate connection to New Zealand. • Instructions received from a customer or beneficial owner since the start of the Russian invasion, requesting action to protect assets or create layers that further obscure beneficial ownership. • Settlors, trustees, directors, or shareholders have no presence on professional platforms such as LinkedIn, or use email addresses from non-professional domains such as Yahoo, Hotmail or Gmail. • Opening several trusts or accounts with the same beneficiary or declaring a different business as the source of funds for each trust, to avoid beneficial ownership thresholds. • During on-boarding, customer asks detailed questions about sanctions, AML/CFT or tax compliance matters, including the application of New Zealand's beneficial ownership transparency, customer due diligence or reporting requirements. • A customer is: reluctant to share information (including data, information and documents); avoiding personal contact; insisting on using an intermediary; avoiding communication after the initial incorporation; or is non-responsive to CDD/ECDD requests
Changing beneficial and effective ownership of assets	• Changes to the beneficial ownership of corporate structures to nominee directors/shareholders, prior to, or shortly after sanctions taking effect. • Changes to ownership of a corporate holding to reduce ownership levels to below the 50% threshold, shortly before or after sanctions designations. • Sanctioned entities may still be able to initiate undue influence through associates or existing corporate governance, or through a joint arrangement with an associate or another sanctioned entity in the ownership chain. • Ownership of a luxury asset via a trust structure, overseen by a trust company and trustee, for no legitimate reason. • Ownership transfers to previously unknown individuals, where that person's economic consumption, displays of wealth or financial footprint (such as private jets, large and/or multiple residences and fleets of luxury cars) does not correspond with their reported wealth.

	• New equity ownership secured by long-dated loan to former equity owners. • Multiple beneficial ownership changes synchronised with new sanctions designations.
Corporate entities obfuscating identities and activities	• Use of aliases and transliteration of company names. • Use of subsidiaries or branches. • Use of third-country nationals in corporate ownership structures. • Registering in jurisdictions with opaque corporate registers where information on ultimate beneficial ownership is not easily accessible. • Beneficial ownership changes to just below allowable thresholds.
Using relatives and close associates	• Assets/funds previously associated with a sanctioned entity are moved by a family member and then disbursed offshore through loosely regulated or Russia-friendly jurisdictions. • Transferring assets, such as shareholdings in holding companies, to trusted proxies such as relatives or employees • Selling or transferring assets at a loss to relatives or close associates, in order to realise their value before sanctions take effect. • Divesting investments to ensure ownership stakes are below a 50% threshold, or relinquishing previous controlling stakes. • Russian high-net worth individuals who are already on international sanctions lists or who anticipate that they may become a sanctions target, transferring assets to family members and/or close associates • Use of banks and financial organisations owned by close associates of a sanctioned entity.

Using real estate to hold value and benefit from wealth	• Russia-linked individuals and entities increasing real-estate transactions, including in higher risk jurisdictions. • Purchase, sale, donation, or legal ownership transfer of high-value real estate in the name of a foreign legal entity with obscure beneficial ownership, particularly where the transaction is not market value or is all-cash, or where transactions involve complex trust or company structures • Use of legal entities or arrangements that may have a connection to sanctioned persons and associates, to hide the ultimate beneficiary or the origins or source of the funds. • Using a non-New Zealand (particularly Russian) bank to pay for an all-cash deposit or settlement, especially if the wired funds come from an account not held by the original requestor. • Dilution or transfer of real estate interests to an individual not affiliated with the buyer or seller. • Maintenance, purchase, or termination of real estate insurance by persons with a known connection to sanctioned persons and their associates.
"Special purpose projects" and FSS/FSB certification	• Transactions involving entities whose website or business registration states the entities work on "special purpose projects." The phrase "special purpose projects" is a Russian designation that typically means for military use • Transactions involving companies that display a certificate from the Russian Federal Security Service (FSS/FSB), which allows these companies to work on high security projects.

3.3 Financial systems

Common technique	Red flags
Using banking and financial systems	• Anomalous increases in the volume or value of orders • Inconsistencies between items ordered and customer's line of business. • Transactions involving financial institutions in jurisdictions that are distinct from company registration and loosely regulated or that support Russia • Payments from venture capital and private equity vehicles located in jurisdictions that support the Russian government, eg Middle East or East Asia. • Non-routine foreign exchange transactions that may indirectly involve sanctioned Russian financial institutions, including transactions that are inconsistent with activity prior to Russian invasion. • Customers overly focused on establishing an appearance of legitimacy via unnecessary or anomalous financial services
Hiding assets and funds	• Repeated transactions that deviate from normal patterns of business, or involve unusual terms and conditions with the same counterparty. • Multiple transactions beneath threshold limits to avoid triggering alerts or attracting attention. • Unconventional or non-standard payment methods in trade transactions - including third-party payments, cash transactions, or cryptocurrencies. • Convoluted transaction structures involving numerous intermediaries, including shell companies and transit accounts. • Transactions by shell companies based in loosely regulated or higher risk jurisdictions e.g. Swiss bank accounts, British Virgin Islands or Cypriot legal persons to disguise the source of funds • Inconsistent or incomplete documentation, such as discrepancies in trade, financial, or shipping documents. • Transactions involving art, precious metals, precious stones, and jewellery trading companies in Asia, and firms with a connection to sanctioned persons and associates. • Transactions involving large amounts of cash, especially in currencies not typically used. • Transactions involving persons not concerned with recouping their initial investment, or paying a substantially higher price than expected. • Sudden transfers or sale of ownership in high-value assets and goods. • Involvement of law firms based in offshore financial centres that have historically specialised in Russian clientele, or in transactions associated with sanctioned persons and associates.

	• Involvement of transportation service companies that have been owned by, or have a connection to, sanctioned persons or their associates, and that may be used to transport luxury goods and obfuscate their movement.
Using virtual assets where SWIFT is blocked	• Transactions initiated from or sent to IP addresses in Russia, Belarus, neighbouring jurisdictions, non-trusted sources or IP addresses previously flagged as suspicious. • Transactions via virtual currency addresses linked to sanctioned entities or individuals. • Use of unlicensed brokers to off-ramp cryptocurrency sent from Russian services/exchanges to the benefit of unknown third parties, in order to avoid Know Your Customer and reporting thresholds. • Customer has direct or indirect transactional exposure to a virtual currency mixing service or ransomware.

3.4 Maritime transport

Common technique	Red flags
Maritime transport evasion techniques	• Manipulating Automatic Identification Signals (AIS) to mask a vessel's name, identifying number, or next port of call. • Disabling a vessel's AIS (this also known as 'spoofing'). • AIS data shows a vessel engaging in indirect routing or unscheduled detours - particularly if those deviations occur in high-risk areas. • The shipping route is abnormal for the product and destination. • Falsifying the vessel's flag, repeatedly changing the country flagging of a vessel within a short time period, or continuing to use a country's flag after a vessel has been deregistered. • Physically altering a vessel's identifying marks, such as painting over the vessel's name or IMO number. • Transferring cargo to another ship (usually at sea) to conceal sanctioned cargoes, entities, or destinations. STS transfers that take place in high-risk areas or at night are of special concern. • Falsifying cargo and vessel documents, like bills of lading, certificates of origin, invoices, insurance certificates and last ports of call, to conceal goods from a sanctioned origin or sanctioned entity.

4. Sources and references

The following open-source links from international bodies may be useful for understanding more about the global sanctions environment and sanctions evasion.

- FinCEN Provides Financial Institutions with Red Flags on Potential Russian Sanctions Evasion Attempts | FinCEN.gov
- **Alert:** FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts (FinCEN.gov) – June 2022
- **Supplementary alert:** FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts (FinCEN.gov) – May 2023
- Guidance to Address Illicit Shipping and Sanctions Evasion Practices | Office of Foreign Assets Control (treasury.gov)
- Financial Sanctions Evasion Tactics: Russian Elites and Enablers (nationalcrimeagency.gov.uk)
- Special Bulletin on Russia-linked money laundering activities (canada.ca)
- Proliferation financing in Australia national risk assessment 2022 | AUSTRAC
- Red Flag Indicators (bis.doc.gov)
- High-Risk Jurisdictions subject to a Call for Action - June 2023 (fatf-gafi.org)
- Jurisdictions under Increased Monitoring - June 2023 (fatf-gafi.org)
- 2022 Corruption Perceptions Index - Transparency.org

MFAT

MINISTRY OF FOREIGN AFFAIRS AND TRADE
MANATŪ AORERE