ADVISORY NOTE

AUSTRALIAN EXPORT SECTOR, RUSSIAN EVASION METHODS

FIRST PUBLISHED 27 JULY 2023[1] - UPDATED: 12 DECEMBER 2024

This Advisory is produced by the Australian Sanctions Office (ASO) within the Department of Foreign Affairs and Trade (DFAT). This Advisory outlines several sanctions evasion tactics employed by third party intermediaries. The purpose of the Advisory is to assist the export sector in identifying warning signs of sanctions evasion and in implementing appropriate compliance measures to ensure that they are sanctions compliant.

Know the Red Flags

Australian sanctions laws, export controls and restrictive measures, along with those of like-minded countries, deprive the Russian regime of revenue and prevent access to sensitive goods—including dual use goods used to support Russia's forces. A range of actors are actively trying to evade Russia-related sanctions and export controls.

Some of the most common tactics used to evade sanctions include the use of third-party intermediaries or transhipment points to circumvent restrictions, disguising the involvement of Australian designated persons or entities in transactions, and obscuring the true identities of Russian end users.

Sanctions evasion – common red flags

Common red flags that can indicate that a transaction may be an attempt to evade sanctions or export controls include:

- Use of shell companies and other legal arrangements to obscure ownership, source of funds, or countries involved, particularly sanctioned jurisdictions;
- Routing purchases through certain transhipment points commonly used to illegally redirect restricted items to Russia;
- A customer's reluctance to share information about the end use of a product, including reluctance to complete an end-user form;
- Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration;
- Declining customary installation, training, or maintenance of the purchased item(s);
- IP addresses that do not correspond to a customer's reported location data;
- Last-minute changes to shipping instructions that appear contrary to customer history or business practices;
- Payment coming from a third-party country or business not listed on the End-User Statement or other applicable end-user form;
- Use of personal email accounts instead of company email addresses;

[1] Previously named: Russian Evasion – Third country transhipment hubs, shell companies & end users

- Operation of complex and/or international businesses using residential addresses or addresses common to multiple closely-held corporate entities;
- Changes to standard letters of engagement that obscure the ultimate customer;
- Transactions involving a change in shipments or payments that were previously scheduled for Russia;
- Transactions involving entities with little or no web presence;
- Requesting that shipments of controlled items be divided into multiple, smaller shipments (which may be an indicator of an intent to avoid law enforcement detection);
- Transactions where goods could be supplied to a 're-seller' in a transhipment hub and then on-sold to companies who have ties to designated persons or individuals;
- Proposed end use of dual use items is in industry sectors subject to minimal or less stringent oversight; and
- Using aliases for the identities of the intermediaries and end user.

Current and New Customers and End Users

Entities that use complex sales and distribution models may obscure visibility of the ultimate end-users of its technology, services, or products.

Best practices in the face of such risks include screening current and new customers, intermediaries, and counterparties through the Consolidated List as well as conducting risk-based due diligence on customers, intermediaries, and counterparties.

Companies should also regularly consult guidance and advisories from the Australian Sanctions Office and the Russian Elites, Proxies and Oligarchs Taskforce to inform and strengthen their compliance programs.

Minimise your risk

The Australian Sanctions Office advises regulated entities to:

- Report any suspicious or illicit activity, which raises a red flag immediately to the Australian Sanctions Office at: sanctions@dfat.gov.au
- Maintain and update effective, risk-based compliance programs that you can adopt to minimize the risk of evasion. The compliance programs should include management commitment, risk assessment, internal controls, testing, auditing and training. These efforts should empower staff to identify and report potential violations of Australian sanctions and export controls to compliance personnel such that companies can make timely voluntary disclosures to the Australian Sanctions Office. Ideally, compliance programs should include controls tailored to the risks the business faces, such as diversion by third-party intermediaries. Some examples of tailored controls could include:
    - Undertaking Know Your Customer (KYC) procedures – use verifiable date wherever possible (see guidance from AUSTRAC);
    - Considering beneficial ownership of entities – ask questions regarding company structures;

- Being extra careful in dealing with companies for which there is little publicly available information;
- Using trusted intermediaries when entering new or unfamiliar markets;
- Being wary of unsolicited purchasers;
- Regularly monitoring the Consolidated List.

Who must comply with Australian autonomous sanctions laws?

Autonomous sanction laws apply to those conducting activities:

- in Australia;
- by Australian citizens and Australian-registered bodies corporate overseas;
- on board Australian-flagged vessels and aircraft.

The Minister for Foreign Affairs, or the Minister's delegate, may grant a sanctions permit authorising certain activities that would otherwise contravene Australian sanctions laws, if satisfied that it is in the national interest to do so (more information is available at About sanctions).

In addition to Australian autonomous sanctions laws, consideration should also be given as to whether any activity you intend to engage in is subject to other Australian laws or the sanction laws of another country. If so, it is recommended you seek legal advice as to how those laws may impact upon the activity.

Penalties for sanctions offences

Sanctions offences are punishable by:

- For an individual - up to 10 years in prison and/or a fine of 2500 penalty units ($825,000 as of 7 November 2024) or three times the value of the transaction(s) (whichever is the greater).
- For a body corporate – a fine of up to 10,000 penalty units ($3.3 million as of 7 November 2024 or three times the value of the transaction(s) (whichever is the greater).

The offences are strict liability offences for bodies corporate, meaning that it is not necessary to prove any fault element (intent, knowledge, recklessness or negligence) for a body corporate to be found guilty. However, an offence is not committed if a body corporate proves that it took reasonable precautions, and exercised due diligence, to avoid contravening the autonomous sanctions laws.

There are practical steps you can take to ensure you (and/or your business) are in compliance with Australian sanctions laws.

False or misleading information

Australian sanction laws establish serious criminal offences for giving false or misleading information in connection with the administration of a sanction law.

These offences are punishable by up to 10 years in prison and/or a fine of 2500 penalty units ($825,000 as of 7 November 2024).

Other Resources

For the purpose of establishing effective risk-based compliance programs, we recommend you consider guidance on:

- Anti-money laundering/ Counter-terrorism financing (AML/CTF)
- Foreign Bribery
- Modern Slavery