



# ADVISORY TO THE AUSTRALIAN EXPORTS SECTOR ON RUSSIAN EVASION – THIRD COUNTRY TRANSHIPMENT HUBS, SHELL COMPANIES AND END USERS

## 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 transshipment points to circumvent restrictions, disguising the involvement of Australian designated persons or entities in transactions, and obscuring the true identities of Russian end users.

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.

## 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 transshipment 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;
  - 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 transshipment 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](mailto: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 data 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](#).

### **Compliance with Australian Sanctions Laws**


Remember, Australian sanction laws apply broadly, including to activities:

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

### **Offences**

Australian sanction laws establish serious criminal offences for contravening a sanctions measure or a condition of a sanctions permit.

These offences are punishable for individuals by up to 10 years in prison, and/or a fine the greater of 2500 penalty units (\$782,500 as of 1 July 2023) or three times the value of the transaction.



They are punishable for bodies corporate by a fine the greater of 10,000 penalty units ((\$3.13 million as of 1 July 2023) or three times the value of the transaction.

These 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.

### **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 (\$782,500 as of 1 July 2023).

A sanctions permit is taken never to have been granted if false or misleading information was contained in the application for the permit.

### **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](#)

*This document provides a summary only of relevant sanctions laws. It should not be relied upon as a substitute for legal advice. It is your responsibility to ensure you do not contravene sanctions law, including by obtaining your own legal advice.*

