



# Special Bulletin on financial activity associated with suspected sanctions evasion

Under the [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Act](#) (the Act), the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) produces strategic intelligence to provide analytical perspectives on the nature and scope of money laundering, terrorist activity financing, the financing of threats to the security of Canada, and sanctions evasion. This Special Bulletin provides background information relevant to Canada's sanctions regime and aims to inform reporting entities on the characteristics of completed or attempted financial transactions related to suspected sanctions evasion to support their ability to meet expanded obligations under the Act, effective August 19, 2024.

The contents of this Bulletin can be leveraged by reporting entities to identify and assess money laundering, terrorist activity financing, or sanctions evasion risks, apply controls and measures to mitigate these risks, and effectively detect and report suspicious transactions to FINTRAC.

## Recent sanctions-related changes to the Act and its associated Regulations

Canada's [2023 Fall Economic Statement](#) announced the government's commitment to introduce legislative measures aimed at combatting sanctions evasion. These measures permit FINTRAC to use its expertise to develop intelligence products, and, where appropriate, disclose its findings to law enforcement partners in an effort to support law enforcement and the implementation of Canada's sanctions regime. As of August 19, 2024, in addition to longstanding obligations to report transactions where there are reasonable grounds to suspect that they are related to money laundering and terrorist activity financing offences, reporting entities must report transactions suspected to be related to sanctions evasion to FINTRAC.

Reporting entities also have other legal obligations under Canada's sanctions laws and associated regulations with respect to monitoring and reporting of relevant property ownership, export and import of goods and other activity in connection with sanctioned individuals and entities. Reporting entities are encouraged to take steps to know their obligations with respect to Canada's sanctions regime and visit [Global Affairs Canada's website](#) for more information, noting that sanctions are subject to change on short notice.

## Canada's sanctions regime

Sanctions have become an increasingly important element in Canada's foreign policy toolkit and play a crucial role in helping maintain and restore international peace and security, combatting corruption, and promoting respect for human rights.

Canadian sanctions place restrictions on the activities permissible between persons in Canada or Canadians outside Canada and foreign states, individuals, or entities. They can target specific countries, organizations, or individuals and can encompass a variety of measures, including restricting or prohibiting trade, financial transactions or other economic activity between Canada and the target state or its enablers.

Canadian sanctions are imposed under the *United Nations Act*, the *Special Economic Measures Act*, and the *Justice for Victims of Corrupt Foreign Officials Act*. These Acts and their relevant Regulations often include designations, or listings, of individuals and entities, which subject those persons to a dealings ban. Reporting entities can consult the [Consolidated Canadian Autonomous Sanctions List](#), which includes individuals and entities subject to specific sanctions regulations made under the [Special Economic Measures Act](#) and the [Justice for Victims of Corrupt Foreign Officials Act](#). For designations listed under the [United Nations Act](#), the [United Nations Security Council Consolidated List](#) provides a list of entities subject to measures imposed by the United Nations Security Council. Please note that sanctions are subject to change without notice. Reporting entities are encouraged to consult the relevant regulations for the most accurate and up to date information.

Global Affairs Canada is responsible for the administration of Canada's sanctions under the *United Nations Act*, the *Special Economic Measures Act*, or the *Justice for Victims of Corrupt Foreign Officials Act*. The Royal Canadian Mounted Police (RCMP) and the Canada Border Services Agency (CBSA) enforce these statutes and associated regulations. It is the responsibility of all persons in Canada and Canadians abroad to comply with Canada's sanctions regime. All persons in Canada and Canadians outside Canada must disclose the existence of property that is owned or controlled by a designated person, as well as transactions related to that property to the RCMP or to the Canadian Security Intelligence Service (CSIS), depending on the specific sanctions regulation.

### Ministerial Directives

Under Part 1.1 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, the Minister of Finance may:

- Issue directives that require reporting entities to apply countermeasures to transactions coming from or going to designated foreign jurisdictions or entities; and
- Recommend the introduction of regulations to restrict reporting entities from entering into a financial transaction coming from or going to designated foreign jurisdictions or entities.

These authorities allow the Minister of Finance to take steps to protect the integrity and reputation of Canada's financial system from foreign jurisdictions and foreign entities that are considered to present high risks for facilitating money laundering, terrorist financing, sanctions evasion or financing of threats to security of Canada. They include countermeasures for reporting entities that enhance or add to existing obligations.

As of the issuance of this Special Bulletin, Ministerial Directives are currently in force with respect to three jurisdictions also subject to Canadian sanctions: the [Democratic People's Republic of Korea](#), the [Islamic Republic of Iran](#) and [Russia](#).

Consult FINTRAC's website for more information on [Ministerial Directives and transaction restrictions](#).

**Example: Special Economic Measures (Russia) Regulations**

Canada imposed and expanded sanctions related to Russia under the *Special Economic Measures Act* in order to respond to the gravity of Russia's unprovoked and unjustifiable invasion of Ukraine, and grave human rights violations that have been committed in Russia.

These sanctions include an imposition of a dealings prohibition on designated individuals and entities listed in Schedule 1 of the *Special Economic Measures (Russia) Regulations*. It is prohibited for any person in Canada and any Canadian outside Canada to:

- deal in any property, wherever situated, held by or on behalf of a designated individual or entity;
- enter into or facilitate, directly or indirectly, any transaction related to such a dealing;
- provide any financial or other related services in respect of such a dealing;
- make any goods, wherever situated, available to a designated individual or entity;
- provide any financial or related service to, or for the benefit of, a designated individual or entity.

The Regulations also prohibit any person in Canada or any Canadian outside Canada, wherever situated, from engaging in a number of activities. This includes, but is not limited to, the following examples of prohibited activities:

- the export, sale, supply or shipping of certain listed goods—including any financial, technical or other services related the goods—to Russia or to any person in Russia for use in offshore oil, shale oil or Arctic oil exploration and production.
- the import by any person in Canada and any Canadian outside Canada, of a specific list of gold, diamonds, steel and aluminum products from Russia or from any person in Russia; and of a specific list of petroleum products, wherever situated, from Russia or from any person in Russia.
- the export, sale, supply or shipping of any good, wherever situated, or to provide any technology, to Russia or to any person in Russia, should this good or technology be listed under the [Restricted Goods and Technologies List](#).
- the export, sale, supply or shipping of any luxury good listed under the Regulations to Russia or to any person in Russia.
- the import, purchase, or acquisition of arms and related material from Russia or from any person in Russia; as well as the export, sale, supply or shipping of arms and designated goods that could be used to make weapons, wherever situated, to Russia or to any person in Russia.
- the provision of a range of services to the Russian oil, gas and chemical industries, including technical, management, accounting, and advertising services.
- the docking in Canada or passing through Canadian waters of ships registered in Russia or used, leased or chartered, by Russia or those ships linked to designated persons.

Financial transactions associated with causing, assisting or promoting prohibited activities is likewise prohibited under the *Special Economic Measures (Russia) Regulations*.

## **Characteristics of financial transactions associated with sanctions evasion**

Individuals and entities sanctioned by the Government of Canada are likely to deploy established techniques and channels to circumvent sanctions and use alternative financial channels should traditional methods be unavailable to them.

These techniques include the use of intermediary jurisdictions to set up complex networks of shell and front companies (often registered to addresses in offshore financial centres or tax havens) and non-resident bank accounts (generally located in secrecy jurisdictions or those known to cater to customers in sanctioned jurisdictions) as a key feature of sanctions circumvention. Some sanctioned individuals are also known to use trade-based money laundering and other techniques to move, hide, and use assets around the world.

Alternative financial channels—among them, cryptocurrencies and other emerging financial technologies—have also played an important role in sanctions circumvention activities.

### **Use of intermediary jurisdictions**

Sanctioned entities may seek to evade sanctions through various means, including through non-sanctioned financial institutions and financial institutions in other countries. Indicators of financial activity related to sanctions evasion through intermediary jurisdictions can include:

- The involvement of legal firms, including company service providers based in offshore financial centres that have historically specialized in clientele from sanctioned jurisdictions or in transactions associated with Politically Exposed Persons and their associates.
- Particular attention should be paid to jurisdictions previously associated with financial flows from sanctioned jurisdictions that are identified as having a notable recent increase in new company formations.
- Jurisdictions with low barriers to set up shell companies as general trading companies, or free trade zone entities are commonly used for professional money laundering and sanctions evasion.
- Attention should also be paid to entities located in international trade hubs with noted anti-money laundering deficiencies or those known to be used by individuals and entities to circumvent sanctions and export controls.
- Actors seeking to circumvent sanctions and export controls through intermediary jurisdictions have been known to use regional financial and trade hubs such as the United Arab Emirates, Türkiye, China, and Hong Kong, as well as neighbouring jurisdictions that maintain commercial links with sanctioned jurisdictions.

### **Evasion of import and export controls**

Sanctions regulations may prohibit any persons in Canada or any Canadian outside Canada, wherever situated, from engaging in activities related to the import, export, sale, supply or shipping of certain listed goods to a listed individual, entity or sanctioned jurisdiction. Some of these goods may be related to the proliferation of weapons of mass destruction, or may have dual civilian and military and/or nuclear uses. Individuals and entities may seek to evade sanctions and export controls by using the following methods:

- Routing of purchases through jurisdictions known to be used to redirect restricted items to or from sanctioned jurisdictions or geographically proximate to jurisdictions subject to international sanctions. Such intermediary

jurisdictions include United Arab Emirates, Türkiye, China, Hong Kong, and countries of the Commonwealth of Independent States.

- Transactions related to payments for military or nuclear or dual-use goods and technologies from shell or front companies, or those based in jurisdictions known to be commonly used by individuals and entities to circumvent sanctions, such as United Arab Emirates, Türkiye, China, Hong Kong, and countries of the Commonwealth of Independent States.
- Particular attention should be paid to transactions where an entity that previously exported sensitive and/or restricted goods and technologies to a sanctioned jurisdiction begins receiving funds from entities in non-sanctioned jurisdictions, including those with geographic proximity or political and/or cultural links to the sanctioned jurisdiction.
- Use of falsified information on shipping forms, and fraudulent trade finance information, including undervaluing the purchase price of goods, to facilitate the movement of sanctioned commodities.
- Transactions related to the export of high-value goods, such as gold, diamonds and other precious metals and stones, through intermediary jurisdictions with a known connection to sanctioned entities.
- Customers who refuse or are unable to provide details on end-users, intended end-use(s), or company ownership.

## **Use of opaque corporate structures**

Sanctioned individuals and entities are known to use complex networks of corporate structures in various jurisdictions to mask their involvement in the international financial system. Such structures include shell and front companies designed to conceal ownership, sources of funds, and the countries involved in the financial transactions.

Indicators of the use of corporate structures to hide the origin or ownership of property and circumvent sanctions include:

- Extensive use of opaque corporate structures such as limited partnerships, limited liability partnerships and offshore companies such as international business corporations.
- Suspicious shell and front companies, which may lack or have minimal online presence. This may include an absence of company websites showing normal business information such as products and services, contact details, and geographic location.
- Newly created, or previously dormant, companies that begin sending or receiving funds from sanctioned jurisdictions or those linked to sanctioned jurisdictions through financial flows.
- 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.
- Particular attention should be paid to entities that share the same counterparties as those suspected of involvement in sanctions circumvention activity, especially where there is a notable increase in transactions.

## **Non-resident banking**

Entities, including those registered in traditional tax havens, sometimes use financial institutions in jurisdictions distinct from the company's registration (non-resident banking). Indicators linked to non-resident banking include:

- Nested correspondent banking, whereby banks in higher risk jurisdictions, including those known to cater to high-risk clients from sanctioned jurisdictions, hold accounts in lower risk jurisdictions and make international payments via these accounts.
- Correspondent banking, where Canadian financial institutions are used as a transit point for international money laundering. Canadian financial institutions should review correspondent banking relationships and should monitor and report correspondent banking transactions that exhibit the characteristics of sanctions evasion.
- Accounts with financial institutions in jurisdictions associated with Russian financial flows that experience a sudden rise in the value being transferred to their respective institutions or areas, without a clear economic or business rationale.

## **Use of proxies and enablers**

Individuals sanctioned by Canada or its allies may also attempt to hide the ultimate beneficial ownership of assets by transferring legal ownership to other individuals or by using professional enablers to facilitate transactions. Indicators may include:

- Transfer of legal ownership of assets to family members, close associates or other nominees shortly before or soon after sanctions are imposed.
- The use of professionals, such as lawyers or accountants to open bank accounts, send/receive money and create corporate structures for the benefit of a sanctioned individual.
- Sanctioned individuals, or their proxies, may also use real estate purchases to hold value and generate wealth. Sanctioned individuals from Russia have increasingly made use of real estate transactions in other jurisdictions.
- Transactions related to high-value assets, such as real estate or other high-value goods. The purchase of real estate in connection with sanctions evasion may involve: opaque corporate structures, including legal entities or trusts; the use of intermediaries, nominees or straw purchasers, including proxies such as family members or close associates; as well as the use of complicit real estate professionals and law firms. Such actors may use a variety of transaction methods to conceal a property's ultimate beneficial owner. See [FINTRAC's Operational Brief for further indicators of money laundering related to real estate](#).

## **Virtual currencies and other alternative financial channels**

Alternative financial channels—including cryptocurrencies and other emerging financial technologies—may play a role in illicit financial flows related to the proceeds of crime and linked to sanctioned jurisdictions. Those involved in sanctions evasions, similar to criminals and criminal organizations, may use cryptocurrencies as a financial vehicle to conceal the source of the proceeds of crime in order to integrate them into the traditional financial system. Potential characteristics associated with virtual currency transactions linked to sanctions evasion may include:

- A customer's transactions are initiated from or sent to Internet Protocol addresses in sanctioned jurisdictions or neighbouring jurisdictions with weak anti-money laundering or anti-terrorist financing systems.
- A customer's transactions are connected to virtual currency addresses linked to sanctioned entities or individuals that may seek to transfer the proceeds of crime.
- A transaction has direct or indirect transactional exposure to virtual currency exchanges or services located in sanctioned jurisdictions or in high-risk jurisdiction with weak anti-money laundering regulations.
- The use of unlicensed brokers to off-ramp cryptocurrency sent from services/exchanges in sanctioned jurisdictions to the benefit of unknown third parties in order to avoid Know Your Customer and reporting thresholds.

Other [money laundering and terrorist activity financing indicators related to virtual currency transactions](#) are available and may be useful to consider when determining if a suspicious transaction should be reported.

## Reporting Suspicious Transactions to FINTRAC

As of August 19, 2024, reporting entities must submit a suspicious transaction report to FINTRAC if there are reasonable grounds to suspect that a financial transaction that occurs or is attempted in the course of their activities is related to the commission or the attempted commission of money laundering, terrorist financing, or sanctions evasion. These transaction reports are critical to FINTRAC's ability to develop and disseminate financial intelligence.

When reporting a financial transaction to FINTRAC, all information that helps identify the transaction as suspected sanctions evasion activity should be included. This includes detailing information related to the products and/or services involved in the suspicious transactions, including the accounts and addresses involved, particularly if they are linked to jurisdictions associated with the facilitation of financial flows from sanctioned jurisdictions.

Reporting entities should also include any information on the ownership, control, and structure of entities involved in transactions, such as listing the owners, directors, officers and those with signing authority, as well as any information about related persons or entities involved, where possible. Reporting entities should also include all available identifying information and descriptions of any legal entities or arrangements involved or associated with the financial transactions.

For guidance on submitting suspicious transaction reports to FINTRAC, see [Reporting suspicious transactions to FINTRAC](#).

## Contact FINTRAC

- **Email:** [guidelines-lignesdirectrices@fintrac-canafe.gc.ca](mailto:guidelines-lignesdirectrices@fintrac-canafe.gc.ca) (include Special Bulletin FINTRAC-2024-SB002 in the subject line)
- **Telephone:** 1-866-346-8722 (toll free)
- **Facsimile:** 613-943-7931
- **Mail:** FINTRAC, 24th Floor, 234 Laurier Avenue West, Ottawa ON, K1P 1H7, Canada

© His Majesty the King in Right of Canada, 2024.

Cat. No. FD4-36/2024E-PDF

ISBN 978-0-660-71589-6

FINTRAC Special Bulletins provide information related to new, emerging and particularly topical methods of money laundering, terrorist activity financing, the financing of threats to the security of Canada, and sanctions evasion. However, these Bulletins should not be considered legal advice. Please refer to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its associated Regulations for the full description of the reporting entities' obligations.