Financial Transactions and Reports Analysis Centre of Canada
Centre d'analyse des opérations et déclarations financières du Canada
Canada

Reference number: FINTRAC-2025-SB001
July 2025

Special Bulletin on financial activity associated with evasion of counter proliferation sanctions

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 on the nature and scope of money laundering, terrorist activity financing, sanctions evasion, and the financing of threats to the security of Canada.

This Special Bulletin provides background information relevant to financial transactions associated with the suspected evasion of sanctions related to counter proliferation. It informs businesses subject to the Act and the public on the characteristics of completed or attempted financial transactions related to this activity in order to facilitate their detection, prevention, and deterrence.

Proliferation as an evolving threat

Canada is home to advanced industrial and technological capabilities, academic and research institutions, and businesses that are recognized leaders in high-technology sectors such as nuclear energy, biotechnology and life sciences, aerospace, chemicals, and electronics. These strengths make Canada and its businesses a potential target for proliferators.

Proliferation refers to efforts by state and non-state actors, including terrorist organizations, to acquire the goods, technologies, resources and knowledge needed to develop chemical, biological, radiological, and nuclear weapons and high-yield explosives, including their precursors and delivery systems. The risks to international security and stability are heightened by the clandestine efforts of proliferators to procure a range of sensitive and restricted items. Canada's Controlled Goods Program regulates goods within Canada through administration of the Controlled Goods Regulations and the Controlled Goods List found in the *Defence Production Act*. Canada also has export controls to ensure that goods leaving the country do so lawfully and are not sent to countries or entities that would misuse them.

To minimize the risk of detection by authorities, proliferators have increasingly and strategically sought out dual-use items—objects that have both military and civilian purposes—that can be used or modified for the development of weapons of mass destruction. This can complicate efforts to enforce counter proliferation controls as they can be acquired under the pretext of non-military use. The targeting of intangible technology transfers by proliferators may also add further complexity to counter proliferation efforts, as these transfers involve the exchange of knowledge, technical data, and expertise, often through seemingly innocuous means—such as academic collaborations, research partnerships, or professional consultancy—and can be shared across borders almost instantaneously through the Internet and encrypted communications. Additionally, the increasing use of cryptocurrencies and alternative financial channels, which may be used to conceal financial trails and evade scrutiny from authorities, further complicates efforts to detect and control the transfer of sensitive materials.

Role of proliferation financiers and associated procurement networks

The acquisition of resources for the development of weapons of mass destruction by state and non-state actors relies on advanced proliferation financing and related procurement networks, which have become adept at using clandestine techniques to circumvent national and international counter proliferation measures. The Financial Action Task Force (FATF) defines proliferation financing as the risk of raising, moving, or making available funds, other assets or economic resources, or financing, in whole or in part, to persons or entities for the proliferation of weapons of mass destruction. This includes the proliferation of their means of delivery or related material (including both dual-use technologies and dual-use goods for non-legitimate purposes).

As Canada is a source of the goods, technology, information and expertise that proliferators may seek, the illicit networks that procure these goods and provide the necessary financial support may pose a threat to Canada's economic and national security interests and to global security. Proliferation financiers and their associated networks may use various techniques to facilitate their illicit activities and circumvent counter proliferation measures imposed by Canada and its allies, such as sanctions, export and border controls. This includes raising funds to finance the programs to develop weapons of mass destruction, disguising and transferring funds to support the purchase of related materials, and using those funds to procure proliferation-related goods and technologies through international financial and trade systems.

Countering proliferation threats through Canada's sanctions regime

The Government of Canada uses various tools and policies to prevent the proliferation of sensitive materials and technologies to ensure that they do not fall into the wrong hands. As proliferation activities depend on access to funds and financial services to procure, transport and receive illicit goods from across the world, disrupting their financing is essential to halting the spread of weapons of mass destruction. Canada's Minister of Finance can issue directives to reporting entities to apply enhanced measures when dealing with foreign entities and/or foreign states at both the national and sub-national levels. Ministerial Directives are in force for the Democratic People's Republic of Korea (DPRK), the Islamic Republic of Iran, and Russia. In addition to existing anti-money laundering and anti-terrorist financing frameworks, Canada relies on the implementation and enforcement of its sanctions and strategic export control regimes to disrupt threat actors and their networks.

Canadian sanctions place restrictions on the activities permissible between persons in Canada or Canadians outside Canada and foreign states, individuals or entities. They are used to respond to various situations, including international crises, support international peace and security, and enforce international norms and laws. Depending on the situation, sanctions can encompass a variety of measures including arms and related materials embargos, asset freezes, export and import restrictions, financial prohibitions and technical assistance prohibitions. For information on Canada's sanctions regime, consult Global Affairs Canada's website.

Sanctions associated with counter proliferation efforts are imposed under the *United Nations Act*, or on a national (autonomous) basis under the *Special Economic Measures Act*.[1] The Act has 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 also report transactions suspected to be related to sanctions evasion to FINTRAC. Reporting entities can consult FINTRAC's compliance guidance: Report suspected sanctions evasion as well as the Special

[1] For a full list of current Canadian sanctions, see Global Affairs Canada's page on current sanctions imposed by Canada.

Bulletin on financial activity associated with suspected sanctions evasion to support their ability to meet reporting obligations under the Act.

Sanctions can be subject to change without notice. As such, reporting entities are advised to consult the relevant regulations for the most up-to-date and accurate information.

Indicators of financial transactions associated with suspected evasion of counter proliferation-related sanctions

Individuals and entities attempting to circumvent counter proliferation-related sanctions use well-established money laundering methods and channels to evade restrictions and support their proliferation activities.

Proliferators often exploit international trade flows and circumvent import and export controls by employing sophisticated techniques similar to those used in money laundering schemes, particularly trade-based money laundering. This often involves disguising transactions as legitimate trades, exploiting markets with permissive export controls and free trade zones, and using collaborative and business relationships to acquire goods and information for illicit purposes.

Proliferators often rely on the use of complex corporate structures, such as shell and front companies, as well as intermediary jurisdictions and trade finance instruments, among other techniques, to effectively bypass counter proliferation controls. Canada's positive international reputation may also make it an attractive jurisdiction for proliferators who may wish to use Canadian financial and commercial entities to legitimize proliferation-related financial transactions between other international jurisdictions. Such actors may use both witting and unwitting third-parties, including Canadian citizens, in their illicit schemes.

Businesses subject to requirements under the Act—particularly financial institutions—may have visibility into various aspects of export-related financial activities that are undertaken to evade proliferation-related sanctions. Through the provision of services offered to exporters, such as trade financing, reporting entities may have access to critical information, including end-use certificates, export documents, letters of credit and intermediary details. This information offers valuable insights into the nefarious activities of proliferators.

Transaction monitoring, sanctions screening and thorough customer due diligence efforts are crucial tools to combat the evasion of counter proliferation sanctions by designated persons or those acting on their behalf. As required under the Act, effective identification and verification for new clients, along with continuous monitoring of existing client relationships and third-party assessments by reporting entities, are key to effective compliance and risk mitigation efforts against potential evasion of counter proliferation sanctions. Through a comprehensive understanding and assessment of client profiles, businesses subject to requirements under the Act are able to identify transactions that do not fit the established client profile, minimize associated risks and improve their ability to detect and report suspicious activity to FINTRAC. For guidance on verifying the identity of persons and entities, see Methods to verify the identity of persons and entities.

Businesses subject to requirements under the Act must ensure that they apply risk-based approaches to their transaction monitoring and customer due diligence programs. This is critical to Canada's counter-proliferation efforts and the effectiveness of its sanctions regime since list-scanning software and other automated compliance programs, while they are potential tools to support businesses in meeting their obligations under the Act, may not adequately capture financial transactions associated with sanctions evasion. This is attributed to the reality that sanctions can target

specific activities beyond just named individuals and entities, and because sanctioned entities and individuals typically use nominees and hide behind opaque corporate structures to avoid detection. By employing a risk-based approach, businesses subject to the Act can more effectively identify and report suspicious transactions to FINTRAC, ensure compliance, and enhance their ability to detect illicit activities.

In addition to the following indicators and characteristics of suspected sanctions evasions, businesses with reporting obligations under the Act are encouraged to consult the Special Bulletin on financial activity associated with suspected sanctions evasion as well as the Operational alert on the Democratic People's Republic of Korea's use of the international financial system for money laundering/terrorist financing to support their ability to identify transactions associated with the suspected evasion of counter proliferation-related sanctions.

Involvement with jurisdictions of proliferation concern

Activities involving jurisdictions of proliferation or diversion concern, particularly when involving transactions related to the import and/or export of proliferation-sensitive goods and technologies, require enhanced screening to reduce the risk of unwittingly aiding the evasion of counter proliferation-related sanctions. Canada participates in several international regimes that regularly review and publish updated lists of controlled items for export. Canada's Export Control List (ECL) is updated annually to reflect changes agreed to by the regimes. Key jurisdictions of proliferation concern include, but are not limited to, the Democratic People's Republic of Korea, the Russian Federation, and the Islamic Republic of Iran. Businesses subject to the Act should also apply heightened scrutiny to transactions involving or suspected to be associated with jurisdictions at a higher risk of being used to divert funds or goods in support of proliferation activities. These jurisdictions may include regional financial and trade hubs and locations with cultural or economic ties to jurisdictions of proliferation concern.

As international trade payments are primarily settled through correspondent banking relationships, proliferation financing networks seek to exploit the limited visibility on transactions offered by these arrangements. Due to the inherent limited visibility in transactions settled through correspondent banking relationships, Canadian financial institutions are urged to closely examine their correspondent banking relationships and to diligently monitor and report any transactions that may indicate sanctions evasion.

Transactional and behavioural characteristics of these activities include the following:

- Transactions involving an individual or entity designated under the *United Nations Act* and/or the *Special Economic Measures Act* or located in or within close proximity to a jurisdiction of proliferation concern.
- Transactions involving individuals identified in open sources as the spouse, relative or agent of a sanctioned individual under the *United Nations Act* and/or the *Special Economic Measures Act*, who may be used as nominees or proxies.
- Transactions involving entities that are physically co-located with or have shared ownership with an entity listed under the *United Nations Act* or the *Special Economic Measures Act.*
- Transactions involving financial institutions located in jurisdictions with known deficiencies in anti-money laundering or anti-terrorist financing measures, are not signatories to international counter proliferation treaties, or have weak enforcement of export control laws.
- Transactions or financial relationships (such as correspondent banking relationships) between businesses and entities located in jurisdictions of proliferation or diversion concern, or located in/in close proximity to geographic areas controlled by terrorist groups. Particular interest should be paid to electronics companies, import-export businesses, supply chain management companies, holding companies, investments and financial

services firms, shipping, security solutions, engineering, food, machinery, steel, telecommunications and clothing companies.

- Transactions involving entities, including financial institutions, in jurisdictions that neighbour or are sympathetic to sanctioned jurisdictions of proliferation or diversion concern. For example, many North Korean front or shell companies and corporate service providers engaged in proliferation activities are based in China or use Chinese financial institutions to facilitate the movement of illicit funds on behalf of the Democratic People's Republic of Korea, often located in the Chinese provinces of Liaoning and Jilin. Both of these share land borders with the Democratic People's Republic of Korea.
- Transactions involving incoming funds from a jurisdiction of proliferation or diversion concern that are quickly offset by outgoing funds of a similar amount within a short period, directed to an individual or entity involved in a field of proliferation interest.
- Transactions involving individuals known to be employed in a sensitive technological sector with potential access to proliferation-related goods or technologies, whether tangible or intangible. This can include individuals working in high-security laboratories, arms manufacturers and other similar industries.
- Transactions suspected of being related to intangible technology transfers, such as contracts, service/servicing agreements, conferences/seminars/training, investments/joint ventures, research grants/partnerships, or salaries/commissions, involving parties with knowledge or expertise in industries of proliferation interest (e.g., nuclear technology or missile development, high performance computing and encryption technologies) with parties linked to jurisdictions of proliferation concern.
- Transactions involving individuals with an educational background in a field of proliferation interest or having engaged in research or publications on proliferation topics with academic institutions in jurisdictions of proliferation concern.
- Transactions involving a jurisdiction of diversion concern that can be used to conceal the intended end-use or end-user of proliferation-related goods and technologies. These include jurisdictions with lax import and export controls, weak anti-money laundering and anti-terrorist financing frameworks, or with free trade zones or free port areas known to be exploited for proliferation or trade-based money laundering schemes.
- Transactions facilitated by correspondent banks known to conduct payments for proliferation regimes or who have correspondent banking relationships with entities located in jurisdictions of proliferation or diversion concern.
- Correspondent banking transactions involving actors that have shared owners or addresses with companies associated with jurisdictions of proliferation or diversion concern.

Import and export of military, sensitive and dual-use goods and technologies

To evade sanctions, shipments of military and dual-use goods and technologies of proliferation concern are often diverted through complex networks of intermediaries and third-parties, often involving intermediary jurisdictions. These intricate networks conceal the true origin and destination of the goods, making it challenging to trace the trade back to sanctioned entities.

Proliferators often seek to acquire high-quality Western-made goods and technologies to develop weapons of mass destruction programs. Given Canada's geographic proximity and its status as the U.S.'s largest trading partner, Canada is

at risk of being targeted by those seeking U.S.-origin controlled items for transfer to third-parties and ultimately to sanctioned jurisdictions.

Indicators and characteristics of suspected evasion of counter proliferation-related sanctions involving import and/or export of military, sensitive and dual-use goods and technologies of proliferation concern can include the following:

- Transactions involving items controlled under proliferation-related domestic or international export control or restriction regimes, such as dual-use, proliferation sensitive or military goods and technologies. To identify sanctions evasion and/or export control evasion of dual-use goods and technologies of proliferation concern, see FINTRAC's Joint financial intelligence advisory: illegal procurement of dual-use goods by Russian end-users.
- Transactions related to payments for military, nuclear or dual-use goods and technologies from shell or front companies, particularly those based in jurisdictions known to be exploited by individuals and entities to circumvent sanctions.
- Routing of shipments of proliferation-sensitive goods through several third parties across multiple jurisdictions in business lines that do not align or appear incompatible with their stated business model.
- Identifying a customer linked to research institutions that are engaged in developing dual-use goods or technologies and that are subject to domestic or international export control or restriction regulations.
- Routing of shipments of proliferation-sensitive goods through jurisdictions known to be used as transshipment points that redirect or re-export restricted items to or from sanctioned jurisdictions or that are geographically proximate to jurisdictions subject to counter proliferation-related sanctions.

Use of complex corporate structures and proxies for anonymity

Entities involved in proliferation-related activities often use complex corporate structures and intermediaries to conceal their operations and evade detection. They frequently rely on the expertise of designated non-financial businesses and professionals, such as company service providers, lawyers, and accountants, to establish these structures. These corporate entities are often set up in offshore financial centers, including tax havens and secrecy jurisdictions, to minimize transparency and conceal the ultimate beneficiaries.

By leveraging networks of front and shell companies, and intricate corporate arrangements, these actors may attempt to hide their true identities, the origin of funds, and the end-users of sensitive goods and technologies. Recognizing these sophisticated methods is crucial for disrupting proliferation financing and ensuring compliance with international sanctions.

Indicators of the use of corporate structures and intermediaries to circumvent proliferation-related sanctions include the following:

- Transactions involving suspected shell and front companies, which may lack or have minimal online presence, have overly generic and non-descriptive names, and share directors and management, addresses, emails, phone numbers and financial infrastructure with other entities in their networks.
- The involvement of third-party nationals as directors, shareholders and other prominent positions in ownership structures of corporate entities to conceal the connection between designated individuals or entities and sanctions activities. For instance, the Democratic People's Republic of Korea has been known to use Chinese nationals for such purposes, effectively masking the true ownership and control of assets to evade international sanctions.

- Transactions related to the procurement of proliferation sensitive and dual-use goods and technologies that involve complex networks of intermediaries, including front companies and shell companies, to conceal end-use and end-user of shipments.
- Transactions related to trade involving suspected front or shell companies in intermediary jurisdictions of proliferation concern wherein both the buyer and consignee of a shipment appear to be shell companies.
- The incorporation of companies in jurisdictions with close geographic proximity to sanctioned jurisdictions. For instance, front and shell companies operating on behalf of the Democratic People's Republic of Korea are commonly registered in China's Liaoning province and specifically the municipalities of Dalian, Dandong, Jinzhou and Shenyang, which border the Democratic People's Republic of Korea. Corporate structures linked to the Democratic People's Republic of Korea are also commonly registered in Hong Kong, an activity facilitated by corporate service providers.

Trade finance instruments and falsified, misrepresented or fraudulent trade documentation

Trade finance is a common vehicle used for proliferation financing. Proliferation financiers and their associated networks often use trade financing instruments to facilitate their nefarious activities, and financial institutions involved in providing trade finance may have access to information relevant to identifying potential suspicious activity. Canadian businesses, such as financial and shipping entities, could become indirectly or unwittingly involved in proliferation networks by facilitating the movement of funds and goods involved in proliferation. The use of fraudulent, altered or misleading trade documentation (i.e., bills of lading, certificates of origin, invoices, packing lists, which typically accompany a shipping transaction) can conceal the origin of funds and end-user of sensitive goods of proliferation concern.

Common transactional and behavioural characteristics of this activity include the following:

- Trade documentation for shipments wherein the description of goods involved is vague or otherwise misrepresented, including false, misleading or non-specific description of goods on trade or financial documentation (e.g., "samples", "machines", and "for business purposes").
- Payments for exports from a third-party not identified on the original letter of credit or other trade documentation, located in an intermediary jurisdiction unrelated to that of the importer of exporter, or in a jurisdiction known to be a potential transshipment point for exports to jurisdictions of proliferation concern.
- Inconsistencies between information contained in trade documents and financial flows such as names, addresses and destinations, including discrepancies related to the goods on trade documentation compared to the actual goods, and discrepancies between invoicing and shipping documentation, involvement of unexplained third-parties, last minute changes in shipment destinations and the types of goods being shipped.
- Trade documentation that lacks details on end-use and end-user of shipments or that lists freight forwarding companies, banks or residential addresses as the end-user.
- Transactions involving the shipment of goods that are inconsistent with normal geographic trade patterns (i.e., country involved does not normally export or import the types of goods being sent).
- Transactions for shipments that are incompatible with the technical level of the country to which it is being shipped (e.g., semiconductor manufacturing equipment shipped to a jurisdiction with no electronics industry).

- Trade finance documentation that indicates an indirect route of shipment or financial transactions where the transaction structure and/or shipment route appears unnecessarily complex or designed to conceal the nature of the transactions.
- Trade finance documentation that indicates that the declared value of the shipment is under or overvalued when compared to the shipment cost or where the values listed make little economic sense, or wherein the transport of goods does not align with the goods being shipped.
- Transactions involving import and export companies that trade with partners in unlikely industries or locations, or that do not align with their business profile (e.g., food exporters trading with electronics manufacturing companies).
- Evidence that documents or representations related to shipping, customs, or payment are falsified or fraudulent, including trade documentation that appears illogical, altered or fraudulent, or documentation that is absent despite being expected for the nature of the trade.
- Trade documentation that indicates that individuals and entities involved are linked or are similar to those listed under sanctions or trade controls, such as addresses, directors, owners, phone numbers, and other contact information.
- Payments for shipments made entirely within a single financial institution, typically involving the transfer of funds from one deposit account to another.
- The use of open account trade, where the terms and conditions of the transaction are only known to the importer and exporter, and is susceptible to abuse by proliferators by limiting the visibility of financial institutions into the underlying activities and documentation of the transactions they process.

Virtual currencies and underlying financial technology

Virtual currencies are used to circumvent Canadian and international counter proliferation-related sanctions as proliferation financiers and their associated networks benefit from the pseudo-anonymous nature of these alternative financial instruments. Money service businesses dealing in virtual currencies are required to fulfill specific obligations as required by the Act and associated Regulations, including those related to client identification.

Virtual currencies are both a tool for obtaining funds to support proliferation activities—such as in the case of the Democratic People's Republic of Korea's financing of its weapons of mass destruction and ballistic missile programs through hacking virtual currency exchanges and decentralized finance platforms—and for the movement of funds, allowing proliferation actors such as the Democratic People's Republic of Korea, Iran and Russia, to evade the traditional financial system.

Potential characteristics associated with virtual currency transactions linked to the evasion of counter proliferation-related sanctions may include the following:

- A customer's transactions are initiated from or sent to beneficiaries with Internet Protocol addresses in sanctioned jurisdictions or neighbouring jurisdictions of proliferation concern.
- A transaction has direct or indirect transactional exposure to virtual currency exchanges located or registered in sanctioned jurisdictions, jurisdictions of proliferation concern, geographic areas that are controlled by or are in close proximity to areas controlled by terrorist organizations, or in high-risk jurisdiction with known anti-money laundering and anti-terrorist financing deficiencies.

Example: Democratic People's Republic of Korea's use of cyber-enabled crimes and virtual currencies to finance weapons of mass destruction and ballistic missile development programs

In February 2021, the U.S. Department of Justice announced that a dual Canadian-American citizen pled guilty to money-laundering on behalf of various criminal schemes, among them the laundering of stolen funds from hacking by North Korean cyberattacks. According to court documents, the individual and his co-conspirators used business email compromise schemes, ATM cash-outs and bank cyber-heists to steal money from victims resulting in the theft of over USD $1.3 million from cryptocurrency wallets. These funds were then laundered through bank accounts and digital currency.

According to the United Nations Panel of Experts, the Democratic People's Republic of Korea relies on such cyber-enabled crimes—as well as hacking cryptocurrencies exchanges, decentralized finance protocols, ransomware attacks, and others—to generate revenue for its weapons of mass destruction and ballistic missile development programs. From 2019 to 2020 alone, an estimated USD $316.4 million worth of virtual assets were stolen by the Democratic People's Republic of Korea.

- A customer sends funds to or receives funds from virtual currency exchanges known to have deficient anti-money laundering and anti-terrorist financing compliance procedures, are located in high-risk jurisdictions, or are known to facilitate transactions in jurisdictions of proliferation concern.
- A transaction has direct or indirect sending and/or receiving exposure from a virtual currency address, wallet, or cluster that is associated with sanctioned entities or individuals, or with facilitating sanctions evasion for jurisdictions of proliferation concern. Particular attention should be paid to customers that also have direct or indirect sending and/or receiving exposure to darknet marketplace, gambling platforms, peer-to-peer platforms and mixers.
- A customer engages in excessive chain hopping (i.e., exchanging virtual assets between different blockchains without trading through a centralized exchange) to exchange more volatile virtual assets (e.g., BTC or ETH) for stablecoins (particularly those pegged to the U.S. dollar such as USD Tether and USD Coin).
- A transaction involves virtual currency exchanges that are known to engage in high-volume trading involving fiat currencies associated with sanctioned jurisdictions or jurisdictions of proliferation concern.
- A customer engages in behaviour that suggests efforts to obfuscate activity on the blockchain—such as chain-hopping, cross-chain bridges, pass-through transactional activity or transfers that otherwise seem to lack economic purpose—and appears to be associated with sanctioned entities, individuals and/or jurisdictions.
- A customer, whose transactions involve interactions with mixing services that are sanctioned, has engaged in transactions with entities located in sanctioned jurisdictions, or that are designated by Canadian or international sanctions regimes in association with counter proliferation efforts.

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

Reporting entities play a key role in Canada's counter proliferation financing efforts. Under the Act, 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 is related to the commission or the attempted commission of money laundering, terrorist financing or sanctions evasion offence. These transaction reports are critical to FINTRAC's ability to develop and disseminate financial intelligence related to proliferation financing and to disrupt the financial flows available to proliferators.

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 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 include any available 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 (include Special Bulletin FINTRAC-2025-SB001 in the subject line)
- **Telephone**: 1-866-346-8722 (toll free)
- **Mail**: FINTRAC, 24th Floor, 234 Laurier Avenue West, Ottawa ON, K1P 1H7, Canada

Cat. N°. FD4-42/2025E-PDF
ISBN 978-0-660-75156-6

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