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

Reference number: SIRA-2023-009
May 2023

Special Bulletin on Russia-linked money laundering activities

Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) produces strategic intelligence on the nature and scope of money laundering and terrorist activity financing. This Special Bulletin provides background and updated information relevant to Russia-linked money laundering. It aims to inform reporting entities on the characteristics of completed or attempted financial transactions related to the laundering of the proceeds of crime. It updates and replaces the previous bulletin on Russia-linked money laundering related to sanctions evasion published in March 2022.

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

Background

On February 24, 2022, Russian forces initiated an unjustified and illegal invasion of Ukraine. Russian attacks over the last year have caused widespread devastation of Ukrainian infrastructure and property, and unnecessary deaths of Ukrainian nationals, including high numbers of civilians.

Canada, in coordination with its partners and allies, has imposed a significant number of new sanctions on Russia-linked individuals and entities in response to Russia's egregious violation of international law and the rules-based international order.

Russia-based individuals and entities sanctioned by the Government of Canada, particularly those whose financial assets have been acquired through corruption and other illegal activity, are likely to deploy established money laundering techniques and channels to evade sanctions and to use alternative financial channels to move financial assets outside of Russia should traditional methods be unavailable to them.

In addition to sanctions measures imposed under the Special Economic Measures Act (SEMA), Canada also advocated strongly for the European Union to remove Russian banks from the Society for Worldwide Interbank Financial Telecommunications (SWIFT), a payment-messaging system used by more than 11,000 financial institutions around the world. Eight* Russian banks have subsequently been removed from the system.

*As of March 2023

Financial transactions in the context of Canada's sanctions landscape

The *Special Economic Measures (Russia) Regulations* consist of a dealings ban on listed individuals and entities, as well as prohibitions on specified goods and financial, technical or other services related to those goods. The regulations also impose restrictions on certain sectors, such as the financial, defence and energy sectors, and impose broad prohibitions on ships associated with Russia or Russian companies from docking in or passing through Canada.

In most cases, the dealings ban restricts persons in Canada and Canadians outside Canada from engaging in activity related to any property of listed persons or providing financial or related services to them. It is important to note that a number of Russian financial institutions are listed in these regulations and it is therefore prohibited for Canadians to engage in certain transactions (including payments and fund transfers) with these listed entities.

To determine whether an individual or entity is a listed person, the Consolidated Canadian Autonomous Sanctions List is available for ease of reference. The consolidated list includes individuals and entities subject to specific sanctions regulations made under the SEMA and the Justice for Victims of Corrupt Foreign Officials Act (JVCFOA). While listings under the JVCFOA are not made in reference to a specific country, a number of Russian foreign nationals are listed, which may have implications for certain activities or transactions. However, please note that the inclusion of the names on this list is for administrative purposes only. For accurate information on which provisions from a given sanctions regulation apply to a specific individual or entity, reference must be made to the relevant regulations in which that individual or entity is listed**.**

Global Affairs Canada is responsible for the administration of Canada's sanctions under the JVCFOA, SEMA and United Nations Act. The Royal Canadian Mounted Police (RCMP) and the Canada Border Services Agency enforce these statutes and associated regulations. All Canadians must disclose to the RCMP the existence of property that is owned or controlled by a designated person, as well as any proposed transactions related that property. Voluntary and mandatory disclosures, particularly from Canadian financial institutions, enhance the effectiveness of Canadian sanctions.

Russia has attempted to circumvent these measures by promoting the use of its home-grown alternative to SWIFT, the System for Transfer of Financial Messages (Система передачи финансовых сообщений) better known as SPFS, which was developed in 2014 after Russia's invasion of Crimea. Russia's central bank claimed in September 2022 that 50 financial institutions had joined SPFS in the previous year, taking the total number of members to 440.

Characteristics associated with a higher risk of exposure to Russia-linked money laundering activities

FINTRAC analysis has highlighted the continued 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 Russian-speaking customers) as a key feature of Russia-linked money laundering methodologies.

Alternative financial channels—among them, cryptocurrencies and other emerging financial technologies—have also played an important role in Russia-linked illicit financial flows related to the proceeds of crime, albeit on a lesser scale.

Opaque corporate structures, high-risk jurisdictions and non-resident banking

Russian entities and individuals seeking to hide the origin or ownership of the proceeds of crime 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 obscure ownership, sources of funds, and the countries involved in the financial transactions. Russia-linked money laundering is also known to use trade-based money laundering and other techniques to move, hide and use assets around the world.

Individuals seeking to launder the proceeds of crime and corruption, particularly those subject to sanctions by Canada or its allies, may also increasingly attempt to hide the ultimate beneficial ownership of assets by transferring legal ownership to family members, close associates and other nominees.

Potential characteristics of suspicious transactions include:

- The involvement of legal firms, including company service providers based in offshore financial centres that have historically specialized in Russian clientele or in transactions associated with Russian elites and their associates.
    - Particular attention should be paid to jurisdictions previously associated with Russian financial flows that are identified as having a notable recent increase in new company formations.
    - Facilitators of Russia-linked illicit financial flows have been known to make extensive use of opaque corporate structures such as limited partnerships (LPs), limited liability partnerships (LLPs) and offshore companies such as international business corporations (IBCs).
- A pattern of shell companies registered in traditional tax havens conducting international wire transfers using financial institutions in jurisdictions distinct from the company's registration (non-resident banking) and associated with Russian financial flows.
    - Nested correspondent banking, whereby banks in higher-risk jurisdictions known to cater to Russian-speaking clients, 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 money laundering.
    - Particular attention should be paid to instances where financial institutions or their intermediaries are connected to the Russian payment system known as SPFS (Система передачи финансовых сообщений (СПФС)).
    - 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.

  - 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.

- Jurisdictions with low barriers to set up shell companies as general trading companies, limited liability corporations (LLCs) or free trade zone entities are commonly used for professional money laundering and sanctions evasion.
  - Particular attention should be paid to entities located in international trade hubs with noted anti-money laundering deficiencies, such as the United Arab Emirates, or in jurisdictions that have seen a recent decline in accountable governance and democratic development, such as Hong Kong.
- Accounts with financial institutions in jurisdictions associated with Russian financial flows that are experiencing a sudden rise in the value being transferred to their respective institutions or areas, without a clear economic or business rationale.
- Since Russia's invasion of Ukraine, Russia-linked individuals and entities have increased the use of real-estate transactions for money laundering purposes, particularly in jurisdictions such as the United Arab Emirates and Türkiye. See FINTRAC's Operational Brief for further indicators of money laundering related to real estate more generally.

Virtual currencies and other alternative financial channels

Alternative financial channels—including cryptocurrencies and other emerging financial technologies—may play a role in Russia-linked illicit financial flows related to the proceeds of crime. Criminals and criminal organizations may use cryptocurrencies as a financial vehicle to obfuscate the source of the proceeds of crime in order to integrate them into the traditional financial system.

Potential characteristics associated with suspicious Russia-linked virtual currency transactions may include:

- A customer's transactions are initiated from or sent to Internet Protocol (IP) addresses in Russia, Belarus, neighbouring jurisdictions with weak anti-money laundering or counter-terrorist financing systems, or other comprehensively sanctioned jurisdictions.
- 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 Russia or in another high-risk jurisdiction with weak anti-money laundering regulations.
- The 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.

Open source analysis of cryptocurrency transactions indicates that Russian entities and individuals represent a disproportionate share of cryptocurrency-enabled crime, including online fraud and ransomware.

Potential characteristics associated with transactions involving the proceeds of ransomware and other cyber-enabled crime may include:

- A customer receives virtual currency from one or more private wallets, and immediately initiates multiple, rapid transfers for alternative virtual currencies (chain hopping) with no apparent related purpose, followed by an immediate withdrawal into fiat currency.
- A customer has direct or indirect transactional exposure to a virtual currency mixing service.
- A customer has direct or indirect receiving transactional exposure to ransomware identified by blockchain analysis tracing software.
- Other indicators related to virtual currency transactions as provided on FINTRAC's website.

Example: U.S. action against Russia-linked Bitzlato as money laundering concern

In January 2023, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued an order that identified the virtual currency exchange Bitzlato Limited as a "primary money laundering concern" in connection with Russian illicit finance. According to the order, Bitzlato plays a critical role in laundering virtual currency by facilitating illicit transactions for ransomware actors operating in Russia, including Conti, a Ransomware-as-a-Service group that has links to the Government of Russia. The same day, the U.S. Department of Justice reported that it had arrested the founder and majority owner of Bitlzato, Russian national Anatoly Legkodymov, in Miami, Florida. He was charged with unlicensed money transmitting for his role in facilitating money laundering through his Hong Kong-based cryptocurrency exchange.

Financial transactions related to sanctions evasion

In addition to anti-money laundering and anti-terrorist financing obligations, reporting entities may have other legal obligations under the Special Economic Measures Act and associated regulations with respect to monitoring and reporting of relevant property and 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 the Canadian Sanctions website for more information.

While sanctions evasion may not constitute a money laundering offence in and of itself, financial transactions with Russia or with entities and jurisdictions engaged in financial activity involving Russia may be at a higher risk of being related to the laundering of the proceeds of crime. As such, reporting entities should undertake greater due diligence associated with such transactions.

Please note that sanctions are subject to change without notice. Additional information is also available on the Sanctions – Russian invasion of Ukraine webpage.

Reporting to FINTRAC

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 an ML/TF offence.

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 SIRA-2023-009 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

FD4-28/2023E-PDF
978-0-660-48348-1

FINTRAC Special Bulletins provide information related to new, emerging and particularly topical methods of money laundering and terrorist activity financing. 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.