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

Reference number: 2022-SIRA-002
March 2022

Special Bulletin on Russia-linked money laundering related to sanctions evasion

Under the *Proceeds of Crime (Money Laundering) and Terrorist Financing 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 and terrorist activity financing. This Special Bulletin provides background and information relevant to Russia-linked money laundering in order to inform reporting entities on recognizing characteristics of completed or attempted financial transactions related to the laundering of the proceeds of crime. It is also possible that money laundering may be connected to the evasion of sanctions measures that have been imposed under the *Special Economic Measures Act* (SEMA).

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

Canada has imposed a significant number of new sanctions in response to the Russian Federation's unprovoked and unjustifiable invasion of Ukraine, with many of these measures undertaken in coordination with Canada's allies and partners.

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 prohibitions restrict persons in Canada and Canadians outside Canada from engaging in any 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**.**

Russia-based individuals and entities sanctioned by the Government of Canada, particularly those whose financial assets have been acquired through illegal activity, are likely to deploy established money laundering techniques and channels to evade sanctions.

In addition to sanctions measures that have been imposed under the SEMA, Canada also advocated strongly for the European Union to remove seven 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.

These actions have prompted speculation that Russian entities might try to circumvent economic measures to enable the continued movement of Russian funds across international borders. This could include an expansion in the use, directly or indirectly, of Russia's alternative to SWIFT, known as SPFS, which was developed in 2014 after Russia's invasion of Crimea.

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 and the Canada Border Services Agency enforce these statutes and associated regulations.

Characteristics associated with a higher risk of Russia-linked money laundering related to sanctions evasion

FINTRAC analysis has highlighted the use of intermediary jurisdictions to setup 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 jurisdictions known to cater to Russian-speaking customers) as a key feature of Russia-linked money laundering methodologies. The attempt to evade sanctions imposed against Russian individuals and entities is likely to be conducted through the same mechanisms.

Sanctions evasion, in and of itself, does not constitute money laundering. In order for money laundering to be present in the context of sanctions evasion, the sanctions evasion would either need to be attempted or committed using proceeds of crime (as defined in the Criminal Code), or the sanctions evasion would need to give rise to or generate proceeds of crime that would then be laundered or attempted to be laundered.

Alternative financial channels—among them, cryptocurrencies and other emerging financial technologies—may also play an important role in Russia-linked illicit financial flows related to the proceeds of crime.

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. 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 limited partnerships (LPs), limited liability partnerships (LLPs) and offshore companies such as international business corporation (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.
    - 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)).
    - 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.
    - 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.
    - Particular attention should be paid to entities with 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, as highlighted by the Financial Action Task Force (FATF), or in jurisdictions that have seen a recent decline in accountable governance and democratic development.
- Accounts with financial institutions or 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.
    - Some Russia-linked individuals and entities have been known to use real-estate transactions for money laundering purposes. 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 Russia-linked illicit financial flows related to the proceeds of crime. Criminal organizations 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, 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 identified by blockchain analysis tracing software related to ransomware.
- Other virtual currency indicators as provided on FINTRAC's website.

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 Canadian Sanctions website for more information.

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 2022-SIRA-002 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

Cat. No. FD4-28/2022E-PDF
ISBN 978-0-660-42726-3

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.