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

OPERATIONAL ALERT

Democratic People's Republic of Korea's Use of the International Financial System for Money Laundering/Terrorist Financing

Reference number: FINTRAC-2017-OA001

Date: December 12, 2017

Operational Alerts provide up-to-date indicators of suspicious financial transactions and high-risk factors related to specific methods of money laundering and terrorist activity financing that are important either because they represent new methods, re-emerging methods or long-standing methods that present a particular challenge.

Dissemination: All reporting entities providing electronic funds transfer services.

Identifying the type of Suspicious Transaction Report: To expedite FINTRAC's disclosure process include the following term in Field G1 Description of suspicious activity of the suspicious transaction report: *DPRK

Background

The purpose of this Operational Alert is to inform Canadian reporting entities of money laundering/ terrorist financing patterns, indicators and risk areas related to the Democratic People's Republic of Korea (North Korea) suspected money laundering and terrorist financing activity.

Following on numerous resolutions of the United Nations Security Council (UNSC) sanctioning both individuals and entities as well as various financial and economic activities,[1] Canada has also implemented sanctions against North Korea. Sanctions related to North Korea have been enacted under the *United Nations Act* and the *Special Economic Measures Act*.[2] The *Regulations Implementing the United Nations Resolutions on the DPRK* implement United Nations Security Council sanctions in relation to North Korea in domestic law.[3] Canada's unilateral sanctions regulations, the *Special Economic*

[1] For UN Security Council Resolutions relating to North Korea, please see: https://www.un.org/sc/suborg/en/sanctions/1718/resolutions.
[2] Further information on Canadian sanctions in relation to the DPRK can be found on Canada's economic sanctions website: http://www.international.gc.ca/sanctions/countries-pays/korea-coree.aspx?lang=eng.
[3] For UN Security Council Resolutions relating to North Korea, please see: https://www.un.org/sc/suborg/en/sanctions/1718/resolutions.

Measures (DPRK) Regulations, include a ban on the provision of financial services to North Korea and to persons in North Korea under the *United Nations Act* and the *Special Economic Measures Act*.[4]

Concurrent to this Operational Alert, FINTRAC has also released a FINTRAC Advisory for reporting entities who have been party to transactions for countries for which the Financial Action Task Force has provided a public statement on serious deficiencies in their anti-money laundering/anti-terrorist financing regime. On November 3, 2017, the Financial Action Task Force (FATF) reiterated its ongoing concern about illicit financing risks related to the North Korea, and thus remains the subject of FINTRAC's Advisory.[5]

[4] For Canadian sanctions currently in force, please see: http://www.international.gc.ca/sanctions/countries-pays/korea-coree.aspx?lang=eng.
[5] 3 November 2017. FATF Statement on the Democratic People's Republic of Korea (DPRK). See: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/statement-dprk-nov-2017.html.

Strategic Context

Due to wide-ranging and comprehensive sanctions against the country, North Korean enterprises have been barred from direct access to the international financial system, including the Canadian financial system. As such, these enterprises often operate through proxies outside of North Korea. The primary goal of these proxies is to facilitate access to both goods and finances, while disguising the role of North Korean individuals and entities as the ultimate initiators or beneficiaries of these transactions.

As the contravention of these sanctions is a predicate crime, any proceeds generated could be laundered. The patterns of activity employed by those seeking to circumvent sanctions against North Korea are also common to other patterns of money laundering and terrorist financing, and thus it may be difficult to distinguish between the evasion of sanctions, and the laundering of the proceeds of the evasion of sanctions.

Reasonable Grounds to Suspect and How to Use Indicators

Criminals disguise their money laundering methods through what they hope will appear to be normal financial transactions in a normal business context. As a result, the decision to submit a suspicious transaction report to FINTRAC (for either a completed or attempted financial transaction) requires more than a "gut feel" or "hunch," although proof of money laundering is not required. Reporting entities are to consider the facts related to a transaction and its context that can, when taken together, give rise to reasonable grounds to suspect that the transaction is related to the laundering or attempted laundering of proceeds of crime. Indicators of money laundering can be thought of as red flags indicating that something may very well be wrong. Red flags typically stem from one or more characteristics, behaviours, patterns and other contextual factors related to financial transactions that make them appear inconsistent with what is expected or considered normal. The review of the trail of indicators may follow various scenarios and lead to different conclusions depending on whether the level of suspicion is strengthened or weakened.

When a reporting entity concludes that another individual, with similar knowledge, experience or training, having reviewed the same material, would likely come to the same conclusion that there are reasonable grounds to suspect that a financial transaction (completed or attempted) is related to illicit funds, then the reporting entity must submit a suspicious transaction report to FINTRAC. The reasons for having reasonable grounds to suspect, as well as the details and facts associated with the indicators that led to those grounds, must be included in the report. The decision to submit a suspicious transaction report requires that a financial transaction be completed or attempted, and that the relevant indicators raise suspicion of money laundering in relation to that transaction. FINTRAC's Guideline 2 on Suspicious Transactions[6] provides more comprehensive guidance and additional indicators that may be useful either as initial triggers or in addition to the indicators listed in this Operational Alert.

The indicators provided in the next section should be considered by reporting entities in order to recognize, assess and report suspicious financial transactions related to DPRK. FINTRAC will use these indicators, along with other sources of information, to assess compliance with reporting obligations. In addition, reporting entities should build and maintain training programs that ensure the submission of high quality suspicious transaction reports on the money laundering of any illicit funds.

Indicators of ML/TF Related to DPRK

The following may be indicative of a financial transaction where there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering or terrorist financing offence related to the laundering of the proceeds of the evasion of sanctions by the DPRK:

Transactions Involving Front or Shell Companies: North Korean entities and individuals have made use of front and shell companies in various jurisdictions to mask their involvement in the international financial system.[7] Such companies may have the following characteristics:

- The lack of their own online presence, such as a company website indicating normal business-related information such as products and services, contact information, and physical geographic location.
- A corporate name which is overly generic, non-descriptive, or easily mistaken with that of another better known corporate entity. Additionally, the corporate name may be regularly misspelled in different ways.
- A pattern of sending or receiving international EFTs to or from Canadian businesses that operate in sectors or industries unrelated to each other.
- Transactional patterns which are exclusively one-directional; e.g., the company only sends but never receives EFTs, or vice versa.

[6] Reference: http://www.fintrac.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.asp
[7] FINCEN. Advisory on North Korea's Use of the International Financial System. FIN-2017-A008. See: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008.

- Transactional patterns in which the same observed activity (e.g., sending EFTs) and the Canadian recipients remain consistent, but the foreign ordering company changes over time, particularly if the sending companies are from the same jurisdiction or geographic area.

Transactions Involving Particular Jurisdictions: North Korean entities and individuals have been observed using particular jurisdictions from which to access the international financial system.[8] While the jurisdictions discussed below are not an exhaustive list, transactions to or from these areas, in combination with other indicators, should be considered when deciding to report a suspicious transaction report to FINTRAC:

- **Liaoning Province, China** shares a land border with North Korea, and both companies and financial institutions in this jurisdiction have been reported to engage in financial activity and other business dealings with North Korean companies and China-based front companies (see Appendix I for a list of cities in Liaoning province).[9] FINTRAC also notes that there is a substantial amount of Canada-linked EFT reporting to a number of these cities, in particular Dalian, China and Shenyang, China.

- **Jilin Province, China** also shares a land border with North Korea, and has been associated with companies employing North Korean guest workers in the food processing and manufacturing sectors.[10] FINTRAC notes that there is also a substantial amount of EFT reporting to Changchun, the capital of Jilin province (See Appendix I for a list of cities in Jilin province).

- **Hong Kong** has also been associated with North Korean financial activity. While this is not unexpected given Hong Kong's role as a major centre of global finance, transactions to or from Hong Kong that display other indicators, particularly those indicating possible use of shell companies, may warrant additional scrutiny.

This Operational Alert provides specific guidance to Canadian reporting entities about indicators and jurisdictions that may be associated with North Korean use of the international financial system for laundering the proceeds of sanctions evasion. While not specifically high risk in and of themselves, transactions originating from or destined for these jurisdictions, when combined with other indicators such as those outlined above, should be considered at elevated risk. In such cases, where reporting entities reach the threshold of reasonable grounds to suspect, they should file suspicious transaction reports or attempted suspicious transaction reports.

[8] FINCEN. Advisory on North Korea's Use of the International Financial System. FIN-2017-A008. See: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008.
[9] FINCEN. Advisory on North Korea's Use of the International Financial System. FIN-2017-A008. See: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008.
[10] http://www.chicagotribune.com/news/nationworld/ct-walmart-aldi-salmon-seafood-north-korea-20171005-story.html.

FINTRAC is reminding all reporting entities subject to the PCMLTFA and its associated Regulations, of their obligations[11] to submit a suspicious transaction report or attempted suspicious transaction report if there are reasonable grounds to suspect that a transaction or attempted transaction is related to a terrorist activity financing (or a money laundering) offence[12].

CONTACT US

Please use "**Operational Alert**" with the **reference number** in the subject heading of your communications with FINTRAC, and in any related STR/TPR reporting to FINTRAC:

- **Email:** guidelines-lignesdirectrices@fintrac-canafe.gc.ca
- **Facsimile:** 613-943-7931
- **Mail:** FINTRAC, 24th Floor, 234 Laurier Avenue West, Ottawa, ON, K1P 1H7
- **Telephone:** 1-866-346-8722 (toll free)

[11] Under section 7 of the PCMLTFA.
[12] Canada. FINTRAC. *Guideline 2: Suspicious Transactions*. http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.asp. June 2017.

Appendix I

Major Cities – Liaoning Province, China

- Shenyang
- Dalian
- Anshan
- Liaoyang
- Fushun
- Dandong
- Jinzhou
- Yingkou

Major Cities – Jilin Province, China

- Changchun
- Jilin City
- Siping
- Liaoyuan
- Tonghua
- Songyuan
- Baicheng
- Yanbian