**Ministerial Directives**

From time to time, the Minister of Finance will issue additional directives for AML reporting entities. The Compliance Officer will ensure that our policies, procedures and Risk Assessment are updated accordingly.

This may include the implementation of new processes in order to comply with directives, and to test the effectiveness of compliance measures. The Compliance Officer will maintain an awareness of such directives by regularly reviewing FINTRAC’s website[[1]](#footnote-1) and subscribing to FINTRAC’s mailing list[[2]](#footnote-2).

Currently, there are ministerial directives pertaining to transactions that originate from, or are destined to North Korea (also known as the Democratic People’s Republic of Korea, or DPRK) and Iran (also known as the Islamic Republic of Iran). Additional information related to Ministerial Directives is provided in the corresponding section below.

# Background

Under Part 1.1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), which came into force on June 19, 2014, 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 Canada’s financial system from foreign jurisdictions and foreign entities that are considered to present high risks for facilitating money laundering and terrorist financing.

The Compliance Officer will maintain an awareness of such directives by regularly reviewing FINTRAC’s website[[3]](#footnote-3) and subscribing to FINTRAC’s mailing list[[4]](#footnote-4).

## Ministerial Directive on the Democratic People’s Republic of Korea (DPRK), Also Known as North Korea

This Ministerial directive requires that all transactions to and from North Korea be treated as high risk, regardless of the amounts of the transactions. In addition, FINTRAC's expectation is that CMTC implements specific measures to mitigate the risk posed by these transactions and document the measures taken.

When conducting these transactions, regardless of the transaction amounts, the measures that taken to mitigate the risk may include:

* keeping a record of all transactions to and from North Korea, regardless of the amount.
  + This record must include details such as the client's name and address, the amount, currency, date and type of transaction.
  + If the client is a person, their date of birth and the nature of their principal business or their occupation, as applicable; and if the client is an entity, the nature of their principal business.
  + If the transaction is an electronic funds transfer, you recording the ordering client and the beneficiary client as well as their addresses, the amount, currency and date of transaction.
  + If the ordering client is a person, their date of birth and the nature of their principal business or their occupation, as applicable; and if the ordering client is an entity, the nature of their principal business.
  + These details must specify whether funds are coming from, or destined to North Korea;
* identifying clients for all transactions and ensuring that the information about the identity of these clients are up to date;
* exercising customer due diligence, including asking for the:
  + source of the funds;
  + purpose of transactions; and
  + beneficial ownership (if the client is an entity);
* conducting enhanced ongoing monitoring of the client and/or the business relationship and/or the account involved in the transaction;
* keeping records of all of the above actions; and
* reporting suspicious transactions (if applicable).

In the case that we suspect, but do not know that a transaction is related to North Korea, the transaction will be treated as high risk. In its Operational Brief[[5]](#footnote-5) on the subject, FINTRAC provides several relevant indicators:

* **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. 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.
  + 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. 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). 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. 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.

Where the facts, context, and indicators lead the Compliance Officer to believe that a transaction may be related to North Korea, the transaction will be reported as suspicious, and the reasons will be noted in the freeform section of the report.

## Ministerial Directive on Financial Transactions Associated with the Islamic Republic of Iran

This Ministerial Directive requires that all transactions originating from or destined to Iran be treated as high risk, regardless of the amounts of the transactions. In addition, FINTRAC’s expectation is that specific measures are implemented to mitigate the risk posed by these transactions, and the measures taken are documented.

When conducting these transactions, regardless of the transaction amounts, the measures that are taken to mitigate the risk may include:

* Keeping a record of all transactions to and from Iran, regardless of the amount.
  + This record must include:
    - Details such as the customer’s name and address, the amount, currency, date and type of transaction.
    - If the customer is a person, their date of birth and the nature of their principal business or their occupation, as applicable; and if the customer is an entity, the nature of their principal business.
    - If the transaction is an electronic funds transfer, recording the ordering customer and the beneficiary, as well as their addresses, the amount, currency and date of transaction.
    - If the ordering customer is a person, their date of birth and the nature of their principal business or their occupation, as applicable; and if the ordering customer is an entity, the nature of their principal business.
* These details must specify whether funds are coming from, or destined to Iran;
* Ensuring that the information about the identity of these customers is up to date;
* Exercising customer due diligence, including asking for the:
  + Source of the funds;
  + Purpose of transactions; and
  + Beneficial ownership (if the client is an entity);
* Conducting enhanced ongoing monitoring of the customer and/or the business relationship and/or the account involved in the transaction;
* Keeping records related to all of the above actions;
* Reporting suspicious transactions (if applicable); and
* Reporting [all other reportable transactions](https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/1-eng) (as applicable).

In the case that we suspect, but do not know that a transaction is related to Iran, the transaction will be treated as high risk. In its Guidance[[6]](#footnote-6) on the subject, FINTRAC provides several relevant indicators:

* Payment for products by electronic funds transfers (EFTs) that include an Iranian originating or destination address;
* Receiving Iranian rial as part of a transaction; or
* Accepting bank drafts or other negotiable instruments that include an Iranian rial component.

For clarity, this does not apply to transactions where there is no suspicion or explicit connection with Iran and there is no evidence of the transaction originating from or being bound for Iran. For example:

* a client whose transactions have previously involved Iran, where the transaction details do not suggest that this transaction is bound for Iran and we are unable to obtain further details about the transaction; or
* the client's identification information is the only suggestion of a connection to Iran (for example, a transaction where the conductor's identification document is an Iranian passport).

Where the facts, context, and indicators lead the Compliance Officer to believe that a transaction may be related to Iran, the transaction will be reported as suspicious, and the reasons will be noted in the freeform section of the report.

1. http://www.fintrac.gc.ca/obligations/directives-eng.asp [↑](#footnote-ref-1)
2. http://www.fintrac.gc.ca/contact-contactez/list-liste-eng.asp [↑](#footnote-ref-2)
3. http://www.fintrac.gc.ca/obligations/directives-eng.asp [↑](#footnote-ref-3)
4. http://www.fintrac.gc.ca/contact-contactez/list-liste-eng.asp [↑](#footnote-ref-4)
5. http://www.fintrac.gc.ca/intel/sintel-eng.asp [↑](#footnote-ref-5)
6. https://www.fintrac-canafe.gc.ca/obligations/dir-iri-eng [↑](#footnote-ref-6)