Money laundering and terrorist financing indicators - Money services businesses

January 2019

This guidance on suspicious transactions is applicable to all money services businesses (MSBs) that are subject to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations. It is recommended that this guidance be read in conjunction with other suspicious transaction report (STR) guidance, including:

- What is a suspicious transaction?
- Reporting suspicious transactions to FINTRAC

This guidance provides money laundering (ML) and terrorist financing (TF) indicators (ML/TF indicators) organized by topic:

- ML/TF indicators related to identifying the person or entity
- ML/TF indicators related to customer behaviour
- ML/TF indicators surrounding the financial transactions in relation to the person/entity profile
- ML/TF indicators related to products and services
- ML/TF indicators based on atypical transactional activity
- ML/TF indicators related to transactions structured below the reporting or identification requirements
- ML/TF indicators involving wire transfers (including electronic funds transfers)
- ML/TF indicators related to transactions that involve non-Canadian jurisdictions
- ML/TF indicators related to use of other parties
- Indicators specifically related to terrorist financing
- ML/TF indicators specific to MSBs

ML/TF indicators are potential red flags that could initiate suspicion or indicate that something may be unusual in the absence of a reasonable explanation. Red flags typically stem from one or more factual characteristics, behaviours, patterns or other contextual factors that identify irregularities related to financial transactions. These often present inconsistencies with what is expected of your customer based on what you know about them.

The ML/TF indicators in this guidance were developed by FINTRAC through a three-year review of ML/TF cases, a review of high quality STRs, published literature by international organizations such as the Financial Action Task Force (FATF) and the

Egmont Group, and consultation with reporting entity sectors. These ML/TF indicators do not cover every possible situation but were developed to provide you with a general understanding of what is or could be unusual or suspicious. On its own, a single ML/TF indicator may not appear suspicious. However, observing an ML/TF indicator(s) could lead you to conduct an assessment of the transaction(s) to determine whether there are further facts, contextual elements or additional ML/TF indicators that require the submission of an STR.

Criminal organizations often combine various methods in different ways in order to avoid the detection of ML/TF. If you detect unusual or suspicious behaviour or a transaction that prompts the need for an assessment, ML/TF indicators combined with facts and context can help you determine if there are **reasonable grounds to suspect** that the transaction is related to the commission or attempted commission of an ML/TF offence. These ML/TF indicators may also be used to explain or articulate the rationale for your reasonable grounds to suspect in the narrative portion of an STR, as they provide valuable information from a financial intelligence perspective.

Important considerations

One piece of the puzzle

The ML/TF indicators in this guidance are not an exhaustive list of ML/TF indicators to support all suspicious scenarios. These ML/TF indicators should be considered as examples to guide the development of your own process to determine when you have reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence. These ML/TF indicators are one piece of the puzzle and are designed to complement your own STR program and can be used in conjunction with other publicly-available ML/TF indicators.

During an assessment, FINTRAC will review your policies and procedures to see how you use ML/TF indicators within your STR program. Part of the assessment will include evaluating how the actual policies follow your documented approach and determining its effectiveness with respect to the use of ML/TF indicators. This can include a review of transactions to determine how your STR program identifies potential STRs and assesses them using facts, context and ML/TF indicators. For example, you can receive questions if you have not reported an STR for a client you have assessed as high risk and that client activity also matches against multiple ML/TF indicators.

Combination of facts, context and ML/TF indicators

If the context surrounding a transaction is suspicious, it could lead you to assess a customer's financial transactions. Facts, context and ML/TF indicators need to be assessed to determine whether there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence. On its own, a single financial transaction or ML/TF indicator may not appear suspicious. However, this does not mean you should stop your assessment. Additional facts or context about the associated individual or their actions may help you reach the reasonable grounds to suspect threshold.

Alert or triggering system

FINTRAC acknowledges that a reporting entity may have developed a system that relies on specific alerts or triggering events to signal when to assess a transaction to determine if an STR should be submitted to FINTRAC. If you rely on such a system, FINTRAC expects that you review the alerts in a timely manner in order to determine if an STR should be submitted. Regardless of how you choose to operationalize these ML/TF indicators, FINTRAC expects that you will be able to demonstrate that you have an effective process to identify, assess and submit STRs to FINTRAC.

General ML/TF indicators

The ML/TF indicators in the following section are applicable to both suspected money laundering and/or terrorist financing. The ability to detect, prevent and deter money laundering and/or terrorist financing begins with properly identifying the person or entity in order to review and report suspicious financial activity.

As an MSB, you may observe these ML/TF indicators over the course of your business activities with a customer. It is important to note that depending on your business activities, some of these ML/TF indicators may not apply.

ML/TF indicators related to identifying the person or entity

The following are examples of ML/TF indicators that you may observe when identifying persons or entities.

- There is an inability to properly identify the customer or there are questions surrounding the customer's identity.
- The customer refuses or tries to avoid providing information required, or provides information that is misleading, vague, or difficult to verify.
- The customer refuses to provide information regarding the beneficial owners, or provides information that is false, conflicting, misleading or substantially incorrect.
- The identification presented by the customer cannot be verified (e.g. it is a copy.).

- There are inconsistencies in the identification documents or different identifiers provided by the customer, such as address, date of birth or phone number.
- Customer produces seemingly false information or identification that appears to be counterfeited, altered or inaccurate.
- Customer displays a pattern of name variations from one transaction to another or uses aliases.
- Customer alters the transaction after being asked for identity documents.
- The customer provides only a non-civic address such as a post office box or disguises a post office box as a civic address for the purpose of concealing their physical residence.
- Common identifiers (e.g. addresses, phone numbers, etc.) used by multiple customers that do not appear to be related.
- Common identifiers (e.g. addresses, phone numbers, etc.) used by multiple customers conducting similar transactions.
- Use of the same hotel address by one or more customers.
- Transactions involve individual(s) or entity(ies) identified by media, law enforcement and/or intelligence agencies as being linked to criminal activities.
- Attempts to verify the information provided by a new or prospective customer are difficult.

ML/TF indicators related to customer behaviour

The contextual information acquired through the know your customer (KYC) requirements or the behaviour of a customer, particularly surrounding a transaction or a pattern of transactions, may lead you to conduct an assessment in order to determine if you are required to submit an STR to FINTRAC. The following are some examples of ML/TF indicators that are linked to contextual behavior and may be used in conjunction with your assessment and your risk based approach.

- Customer makes statements about involvement in criminal activities.
- Customer conducts transactions at different physical locations, or approaches different employees.
- Evidence of untruthfulness on behalf of the customer (e.g. providing false or misleading information).
- Customer exhibits nervous behaviour.
- The customer refuses to provide information when required, or is reluctant to provide information.
- Customer has a defensive stance to questioning.
- Customer presents confusing details about the transaction or knows few details about its purpose.
- Customer avoids contact with reporting entity employees.
- The customer refuses to identify a source for funds or provides information that is false, misleading, or substantially incorrect.

- The customer exhibits a lack of concern about higher than normal transaction costs or fees.
- Customer makes inquiries/statements indicating a desire to avoid reporting or tries to persuade the reporting entity not to file/maintain required reports.
- Insufficient explanation for source of funds.

ML/TF indicators surrounding the financial transactions in relation to the person/entity profile

Clearly understanding the expected activity of a person or entity will allow you to assess their financial activity with the proper lens. For example, an entity involved in an industry that is not normally cash intensive conducting excessive cash transactions or a person conducting financial transactions atypical of their financial profile. The following are some examples of ML/TF indicators surrounding the financial transactions related to person/entity profile.

- The transactional activity far exceeds the projected activity at beginning of the relationship.
- The transactional activity (level or volume) is inconsistent with the customer's apparent financial standing, their usual pattern of activities or occupational information (e.g. student, unemployed, social assistance, etc.).
- The transactional activity is inconsistent with what is expected from a declared business.
- The volume of transactional activity exceeds the norm for geographical area.
- Customer appears to be living beyond their means.
- Large and/or rapid movement of funds not commensurate with the customer's financial profile.
- Rounded sum transactions atypical of what would be expected from the customer.
- Size or type of transactions atypical of what is expected from the customer.
- Conducting transactions when the customer's address or employment address are outside the local service area without a reasonable explanation.
- There is a sudden change in customer's financial profile, pattern of activity or transactions.
- Customer uses notes, monetary instruments, or products and/or services that are unusual for such a customer.

ML/TF indicators related to products and services

Your process to evaluate risk for products and services you provide should be documented as part of your KYC and risk assessment requirements. The following ML/TF indicators will focus on products or services that may be applicable within your business.

- A product and/or service initiated on behalf of a person or entity that is inconsistent based on what you know about that customer.
- Frequent and/or atypical transfers between the customer's products for no apparent reason.

ML/TF indicators based on atypical transactional activity

There are certain transactions that are outside the normal conduct of your everyday business. These transactions may be indicative of a suspicious transaction, and would require additional assessment. Some examples of ML/TF indicators based on atypical transactional activity are listed below.

- A series of complicated transfers of funds that seems to be an attempt to hide the source and intended use of the funds.
- Transactions displaying financial connections between individuals or businesses that are not usually connected (e.g. a food importer dealing with an automobile parts exporter).
- Transaction is unnecessarily complex for its stated purpose.
- Customer presents notes or financial instruments that are packed, transported or wrapped in an uncommon way.
- A customer's transactions have no apparent business or economic purpose.
- Transaction consistent with publicly known trend in criminal activity.
- Customer deposits musty, odd smelling or extremely dirty bills.
- Transaction involves a suspected shell entity (an entity that does not have an economical or logical reason to exist).
- Customer frequently exchanges small bills for larger bills.
- Suspicious pattern emerges from a customer's transactions (e.g. transactions take place at the same time of day).
- Atypical transfers between the customer's products.
- Atypical transfers by customer on an in-and-out basis, or other methods of moving funds quickly, such as a currency exchange followed immediately by a wire transfer of the funds out.
- Funds transferred in and out on the same day or within a relatively short period of time.
- Unusual amount of self-use by agent/owner.

ML/TF indicators related to transactions structured below the reporting or identification requirements

Structuring of transactions to avoid reporting or identification requirements is a common method for committing or attempting to commit an ML/TF offence. There are multiple thresholds which trigger reporting/identification requirements by a reporting entity.

Some examples of ML/TF indicators which may be indicative of a person or entity attempting to evade identification and/or reporting thresholds are listed below.

- You become aware of the structuring of wire transfers at multiple locations.
- Customer appears to be structuring amounts to avoid customer identification or reporting thresholds.
- Customer appears to be collaborating with others to avoid customer identification or reporting thresholds.
- The structuring of wire transfers through multiple locations of the same MSB or by groups of individuals who enter a single location at the same time.
- Multiple transactions conducted below the reporting threshold within a short time period.
- Customer makes inquiries that would indicate a desire to avoid reporting.
- Customer exhibits knowledge of reporting thresholds.
- Customer conducts transactions at different physical locations or with different representatives in an apparent attempt to avoid detection.

ML/TF indicators involving wire transfers (including electronic funds transfers)

In our current global environment, it is increasingly easier to transfer funds to, from or through multiple jurisdictions (municipal, national or international) in a rapid fashion. This presents an increased ML/TF risk as transactions through multiple jurisdictions increases the difficulty for reporting entities and law enforcement to trace illicit funds. Examples of these types of transactions which may require further assessment include the following.

- Customer is unaware of details surrounding incoming wire transfers, such as the ordering customer details, amounts or reasons.
- Customer does not appear to know the sender of the wire transfer from whom the wire transfer was received, or the recipient to whom they are sending the wire transfer.
- Customer frequents multiple locations utilizing cash, prepaid credit cards or money orders/cheques/drafts to send wire transfers overseas.
- The customer sends wire transfers or receives wire transfers to or from multiple beneficiaries that do not correspond with the expected activity of the customer.
- Customer is accompanied by individuals who appear to be sending or receiving wire transfers on their behalf.
- Multiple individuals are sending wire transfers that are similar in amounts, receiver names, security questions, addresses or destination country.
- Customer attempts to specify the routing of an international wire transfer.
- Client conducts wire transfers that do not include theirs or the beneficiary's requisite information.

- Customer utilizes structured cash transactions to send wire transfers in an effort to avoid record keeping requirements.
- Multiple customers have sent wire transfers over a short period of time to the same recipient.
- Large and/or frequent wire transfers between senders and receivers with no apparent relationship.
- Customer sending to, or receiving wire transfers from, multiple customers.

ML/TF indicators related to transactions that involve non-Canadian jurisdictions

There are certain types of transactions that may be sent or received from jurisdictions outside of Canada where there is higher ML/TF risk due to more permissible laws or the local ML/TF threat environment. The following are examples to consider when making an assessment of the financial transaction conducted by a person/entity through your business.

- Transactions with jurisdictions that are known to produce or transit drugs or precursor chemicals or are sources of other types of criminality.
- Transactions with jurisdictions that are known to be at a higher risk of ML/TF.
- Transaction/business activity involving locations of concern, which can include jurisdictions where there are ongoing conflicts (and periphery areas), countries with weak money laundering/terrorist financing controls, or countries with highly secretive banking or other transactional laws such as transfer limits set by a government.
- Transactions involving any countries deemed high risk or non-cooperative by the Financial Action Task Force.
- Customer makes frequent overseas transfers, not in line with their financial profile.

Due to the ever-evolving nature of the ML/TF environment, high risk jurisdictions and trends are often subject to change. To ensure that you are referencing accurate information, FINTRAC encourages you to research publicly-available sources on a regular basis to support these ML/TF indicators as part of your STR program. There are multiple sources that identify jurisdictions of concern, including the FATF which publishes contextual information on high-risk jurisdictions in relation to their risk of money laundering and terrorist financing. You may also observe funds coming from or going to jurisdictions that are reported in the media as locations where terrorists operate/carry out attacks and/or where terrorists have a large support base (state sponsors or private citizens). Identifying high-risk jurisdictions or known trends can also be included as part of your risk based approach and internal STR program.

ML/TF indicators related to use of other parties

In the course of a ‘normal' financial transaction, there are a ‘normal' number of parties who are engaging in the transaction, depending on the nature of the transaction at hand. Transactions that involve parties not typically associated with a transaction can present an elevated risk of money laundering and/or terrorist financing. These additional parties can be used to allow a criminal to avoid being identified or being linked to an asset. This section includes examples of how the involvement of other parties may be indicative of the structure of a criminal enterprise. Some examples of such other parties include the use of a third party, nominee or gatekeeper.

Use of third party

A third party is any individual or entity that instructs someone to act on their behalf for a financial activity or transaction. There are some situations where there is an apparent and discernable rationale for the inclusion of the third party in a transaction and this may not be suspicious. However, you may become suspicious in a situation where the reason for a third party acting on behalf of another person or entity does not make sense based on what you know about the customer or the third party. Use of third parties is one method that money launderers and terrorist financiers use to distance themselves from the proceeds of crime or source of criminally obtained funds. By relying on other parties to conduct transactions they can distance themselves from the transactions that can be directly linked to the suspected ML/TF offence. Some examples of ML/TF indicators related to the use of a third party can be found below.

- A customer conducts transaction(s) while accompanied, overseen or directed by another party.
- Wire transfers to or from unrelated parties (foreign or domestic).
- Customer appears or states to be acting on behalf of another party.

Use of nominee

A nominee is a particular type of other party that is authorized to conduct transactions on behalf of a person of entity. There are legitimate reasons for relying on a nominee to conduct financial activity of behalf of someone else. However, this type of activity is particularly vulnerable to ML/TF as it is a common method used by criminals to distance themselves from the transactions that could be linked to suspected ML/TF offences. The following is an example of ML/TF indicators relating to the misuse of nominees.

- Customer is involved in transactions that are suspicious but refuses or is unable to answer questions related to the transactions.

Use of gatekeeper

A gatekeeper is an individual who controls access to the financial system and can act on behalf of a customer. Such services can be abused so that criminals have access to the financial system without being identified. Gatekeepers may include lawyers, accountants and other professions which can access the financial system on behalf of a customer. While there are many transactions where it is ‘normal' to have a gatekeeper represent the interests of a customer, such an appearance of normalcy can also be utilized to the advantage of criminals to provide the veneer of legitimacy to their transactions. The use of gatekeepers themselves is not an indicator of an ML/TF offence. However, entities should consider the following examples which can indicate misuse of the financial system access provided to gatekeepers.

- Gatekeeper avoids identifying their customer or disclosing their customer's identity when such identification would be normal during the course of a transaction.
- Gatekeeper is willing to pay higher fees and seeks to conduct the transaction quickly when there is no apparent need for such expediency.
- Gatekeeper is processing transactions not typical of their business (e.g. excessive amount of cash, payment to non-customers or parties of transactions).

Indicators related to terrorism financing

In Canada, terrorist financing offences make it a crime to knowingly collect or provide property, which can include financial or other related services, for terrorist purposes. This section is focused on examples that are specific to the possible commission of a terrorist financing offence. However, please note that the other ML/TF indicators in this guidance may also prove relevant in determining when you have reasonable grounds to suspect the commission of terrorist financing as the methods used by criminals to evade detection of money laundering are similar.

Indicators specifically related to terrorist financing:

The indicators below are some examples of indicators relating to terrorist financing.

- Transactions involving certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls.
- Transactions in the name of an entity, a foundation or association, which may be linked or involved with a suspected terrorist organization.
- The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
- Raising donations in an unofficial or unregistered manner.

- Customer identified by media or law enforcement as having travelled, attempted or intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Transactions involve individual(s) or entity(ies) identified by media and/or sanctions lists as being linked to a terrorist organization or terrorist activities.
- Law enforcement information provided which indicates individual(s) or entity(ies) may be linked to a terrorist organization or terrorist activities.
- Customer conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations. Individual or entity's online presence supports violent extremism or radicalization.
- Customer donates to a cause that is subject to derogatory information that is publicly available (e.g. crowdfunding initiative, charity, NPO, NGO, etc.).

ML/TF indicators specific to MSBs

In addition to the general ML/TF indicators that have been highlighted in this guidance, there may be more specific ML/TF indicators related to your MSB, including foreign exchange dealers, money remitters, issuers of traveller's cheques, and agents of the Crown that sell or redeem money orders. Below are some examples of sector specific ML/TF indicators that you should consider as part of your STR program.

- Customer requests a transaction at a foreign exchange rate that exceeds the posted rate.
- Customer wants to pay transaction fees that exceed the posted fees.
- Customer exchanges currency and requests the largest possible denomination bills in a foreign currency.
- Customer knows little about address and contact details for payee, is reluctant to disclose this information, or requests a bearer instrument.
- Customer wants a cheque issued in the same currency to replace the one being cashed.
- Customer wants cash converted to a cheque and you are not normally involved in issuing cheques.
- Customer wants to exchange cash for numerous postal money orders in small amounts for numerous other parties.
- Customer enters into transactions with counter parties in locations that are unusual for the customer.
- Customer instructs that funds are to be picked up by a third party on behalf of the payee.

- Customer makes large purchases of traveller's cheques not consistent with known travel plans.
- Customer makes purchases of money orders in large volumes.
- Customer requests numerous cheques in small amounts and various names, which total the amount of the exchange.
- Customer requests that a cheque or money order be made out to the bearer.
- Customer requests that a large amount of foreign currency be exchanged to another foreign currency.
- Customer purchases a large volume of money orders and changes payment type to avoid reporting requirements.