Money laundering and terrorist financing indicators - Securities dealers

January 2019

This guidance on suspicious transactions is applicable to securities dealers 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 client 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 related to change in account activity
- 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 security dealers

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 client 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 indicatorsare 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 client'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 financial activity.

As a securities dealer, you may observe these ML/TF indicators over the course of your business activities with a client. 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 client or there are questions surrounding the client's identity.
- When opening an account, the client refuses or tries to avoid providing information required by the financial institution, or provides information that is misleading, vague, or difficult to verify.
- The client refuses to provide information regarding the beneficial owners of an account opened for an entity, or provides information that is false, misleading or substantially incorrect.
- The identification presented by the client cannot be verified (e.g. it is a copy).
- There are inconsistencies in the identification documents or different identifiers provided by the client, such as address, date of birth or phone number.
- Client produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Client displays a pattern of name variations from one transaction to another or uses aliases.
- Client alters the transaction after being asked for identity documents.
- The client provides only a non-civic address such as a post office box as an address 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 clients that do not appear to be related.

- Common identifiers (e.g. addresses, phone numbers, etc.) used by multiple clients conducting similar transactions.
- Transactions involve individual(s) or entity(ies) identified by media or law enforcement and/or intelligence agencies as being linked to criminal activities.
- Attempts to verify the information provided by a new or prospective client are difficult.

ML/TF indicators related to client behaviour

The contextual information acquired through the know your client (KYC) requirements or the behaviour of a client, 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 can be used in conjunction with your assessment and your risk based approach.

- Client makes statements about involvement in criminal activities.
- Client conducts transactions at different physical locations, or approaches different employees.
- Evidence of untruthfulness on behalf of the client (e.g. providing false or misleading information).
- Client exhibits nervous behaviour.
- The client refuses to provide information when required, or is reluctant to provide information.
- Client has a defensive stance to questioning.
- Client presents confusing details about the transaction or knows few details about its purpose.
- Client avoids contact with reporting entity employees.
- The client refuses to identify a legitimate source for funds or provides information that is false, misleading, or substantially incorrect.
- The client exhibits a lack of concern about higher than normal transaction costs or fees.
- Client 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.
- Unexplained transfers between the client's products and accounts.
- Unexplained transfers by client on an in-and-out basis, or other methods of moving funds quickly, such as a cash deposit followed immediately by a wire transfer of the funds out.
- Client closes account after an initial deposit is made without a reasonable explanation.

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 receiving excessive cash deposits 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 the time of account opening or the beginning of the relationship.
- The transactional activity (level or volume) is inconsistent with the client'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 (e.g. business account has no normal business-related activities, such as the payment of payrolls or invoices).
- Client appears to be living beyond their means.
- Large and/or rapid movement of funds not commensurate with the client's financial profile.
- Rounded sum transactions, atypical of what would be expected from the client.
- Size or type of transactions atypical of what is expected from the client.
- Opening accounts when the client's address or employment address are outside the local service area without a reasonable explanation.
- There is a sudden change in client's financial profile, pattern of activity or transactions.
- Client uses notes, monetary instruments, or products and/or services that are unusual for such a client.
- Activity in investment account is more typical of a bank account.
- Investment activity is concentrated in microcap stocks/low-priced securities.

ML/TF indicators related to products and services

Accounts can take different forms (e.g. chequing, savings, investment, etc.) and for the purposes of this section the ML/TF indicators below will aim to address the ML/TF risks linked to all types of accounts held by various reporting entities in Canada. There are many ML/TF indicators related to account activity. Your process to evaluate risk for accounts and any other 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.

- Holding multiple accounts at several financial institutions for no apparent reason.
- Suspected use of a personal account for business purposes, or vice-versa.
- Client appears to have recently established a series of new relationships with different financial entities.
- A product and/or service opened on behalf of a person or entity that is inconsistent based on what you know about that client.
- Accounts used for pass-through activities (e.g. to receive and subsequently send funds to beneficiaries).
- Use of multiple foreign bank accounts for no apparent reason.
- The client has multiple products at the same institution for no apparent legitimate purpose.
- Frequent and/or atypical transfers between the client's products and accounts for no apparent reason.

- The same individual(s) holds signing authority for accounts held by multiple entities where there is no legal reason or sufficient explanation for such an arrangement.
- Accounts held by multiple entities either headquartered at the same location or having the same directors/signing authorities for no apparent reason.

ML/TF indicators related to change in account activity

Certain changes regarding an account may be indicative of ML/TF for a multitude of reasons including, but not limited to, the use of an account to suddenly launder or transmit funds, an increase in volume, changes in ownership of an account, etc. Changes in account activity may trigger a need for further assessment of the person or entity holding the account and some examples to consider are listed below.

- A business account has a change in ownership structure with increases in transactional activity and no apparent explanation.
- An inactive account begins to see financial activity (e.g. deposits, wire transfers, withdrawals).
- Accounts that receive relevant periodical deposits and are inactive at other periods without a logical explanation.
- Abrupt change in account activity.

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.
- Client presents notes or financial instruments that are packed, transported or wrapped in an uncommon way.
- A client's transactions have no apparent business or economic purpose.
- Transaction consistent with publicly known trend in criminal activity.
- Client 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).
- Suspicious pattern emerges from a client's transactions (e.g. transactions take place at the same time of day).
- Funds transferred in and out of an account on the same day or within a relatively short period of time.

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 deposits at multiple branches or institutions.
- Client appears to be structuring amounts to avoid client identification or reporting thresholds.
- Client appears to be collaborating with others to avoid client identification or reporting thresholds.
- The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.
- Multiple transactions conducted below the reporting threshold within a short time period.
- Client makes inquiries that would indicate a desire to avoid reporting.
- Client conducts transactions at different physical locations or with different representatives in an apparent attempt to avoid detection.
- Client exhibits knowledge of reporting thresholds.

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 accounts and/or 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.

- Client is unaware of details surrounding incoming wire transfers, such as the ordering client details, amounts or reasons.
- Client 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.
- Client frequents multiple locations utilizing cash, prepaid credit cards or money orders/cheques/drafts to send wire transfers overseas.
- The client sends wire transfers or receives wire transfers to or from multiple beneficiaries that do not correspond to the expected use of the account type or business account.
- Client is accompanied by individuals who appear to be sending or receiving wire transfers on their behalf.
- Client 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.
- Client utilizes structured cash transactions to send wire transfers in an effort to avoid record keeping requirements.
- Funds are deposited or received into several accounts and then consolidated into one before transferring the funds outside the country.
- Immediately after transferred funds have cleared, the client moves funds, to another account or to another individual or entity.
- Multiple clients have sent wire transfers over a short period of time to the same recipient.
- Large wire transfer or high volume of wire transfers are conducted or received through the account that does not fit the expected pattern of that account.
- Large and/or frequent wire transfers between senders and receivers with no apparent relationship.
- Client sending to, or receiving wire transfers from, multiple clients.

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.

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. For example, in the instance of depositing cash to a personal bank account, there is generally one party to the transaction: the individual who holds the account depositing into their own account. In contrast, with the deposit of cash to a business account, you can have many different roles that may be expected, including: Individuals associated with the business's finance function holding authority over the account, while another employee may be charged with depositing the cash.

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 or account. 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 intermediary.

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 client 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.

- Multiple deposits which are made to an account by non-account holders.
- Unrelated parties sending email money transfers or other forms of electronic transfers to the same beneficiary with no apparent relation to the recipient or no stated purpose for the transfers.
- A client conducts transaction while accompanied, overseen or directed by an unrelated party.
- A client makes numerous outgoing payments to unrelated parties shortly after they receive incoming funds.
- Wire transfers, deposits or payments to or from unrelated parties (foreign or domestic).
- Client appears or states to be acting on behalf of another party.
- Account is linked to seemingly unconnected parties.

Use of nominee

A nominee is a particular type of other party that is authorized to open accounts and 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. These are some examples of ML/TF indicators relating to the misuse of nominees.

- An individual maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- An individual or entity other than the stated account holder conducts the majority of the transaction activity which seems unnecessary or excessive.
- Client is involved in transactions or account activity that are suspicious however refuses or is unable to answer questions related to the account or transactions.
- Client is involved in transactions that are suspicious but appears unaware of being involved in possible money laundering activities.

Use of intermediaries

An intermediary is an individual or entity that controls access to the financial system and can act on behalf of a client. Such services can be abused so that criminals have access to the financial system without being identified. Intermediaries may include lawyers and other professionals who can access the financial system on behalf of a client and are not otherwise subject to the requirements of the PCMLTFA. While there are many transactions where it is ‘normal' to have an intermediary represent the interests of a client, 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 an intermediary is not an indicator of an ML/TF offence. However, reporting entities should consider the following examples which can indicate misuse of the financial system access provided by intermediaries.

- Intermediary avoids identifying their client or disclosing their client's identity when such identification would be normal during the course of a transaction.
- Intermediary is willing to pay higher fees and seeks to conduct the transaction quickly when there is no apparent need for such expediency.
- Intermediary is utilizing its account for transactions not typical of its business (e.g. pass through account, excessive amount of cash, payment to non-clients or parties of transactions).
- Apparent misuse of correspondent accounts by intermediary to obscure the origin and/or destination of funds.

Indicators associated 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 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.
- An account opened 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.
- Client 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.
- Client 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.
- Client donates to a cause that is subject to derogatory information that is publicly available (e.g. crowdfunding initiative, charity, NPO, NGO, etc.).
- Client provides multiple variations of name, address, phone number or additional identifiers.

ML/TF indicators specific to securities dealers

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 business of dealing in securities, segregated fund products or any other financial instruments, including portfolio managers and investment counsellors. Below are some examples of sector specific ML/TF indicators that you should consider as part of your STR program.

- Accounts that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the client or their financial ability.

- Any dealing with a third party when the identity of the beneficiary or counter-party is undisclosed.
- Client attempts to purchase investments with cash.
- Client wishes to purchase a number of investments with money orders, traveller's cheques, cashier's cheques, bank drafts or other bank instruments, especially in amounts that are slightly less than $10,000, where the transaction is inconsistent with the normal investment practice of the client or their financial ability.
- Client uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time and such activity is inconsistent with the normal investment practice of the client or their financial ability.
- Client wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account which is inconsistent with the normal practice of the client.
- Client frequently makes large investments in stocks, bonds, investment trusts or other securities in cash or by cheque within a short time period, inconsistent with the normal practice of the client.
- Client makes large or unusual purchases of securities in cash.
- The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading.
- Transfers of funds or securities between accounts not known to be related to the client.
- Several clients open accounts within a short period of time to trade the same stock.
- Client is an institutional trader that trades large blocks of junior or penny stock on behalf of an unidentified party.
- Unrelated clients redirect funds toward the same account.
- Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity.
- Transaction of very large dollar size, in contrast with what you know about your client.
- Client is willing to deposit or invest at rates that are not advantageous or competitive.
- All principals of client are located outside of Canada.
- Client attempts to purchase investments in the name of a third party.
- Payments made by way of third party cheques are payable to, or endorsed over to, the client.
- Transactions made by your employees, or that you know are made by a relative of your employee, to benefit unknown parties.
- Third-party purchases of shares in other names (i.e., nominee accounts).
- Transactions in which clients make settlements with cheques drawn by or remittances from, third parties.
- Purchasing unusually large amounts of securities or stock certificates in the names of individuals other than the client.
- Client maintains bank accounts and custodian or brokerage accounts at offshore banking centres with no explanation by client as to the purpose for such relationships.
- Proposed transactions are to be funded by international wire payments, particularly if from countries where there is no effective anti-money-laundering system.

Date Modified:

2021-01-04