COMPLIANCE PROGRAM

ANTI-MONEY LAUNDERING AND ANTI-TERRORISM FINANCING

Compliance Officer: KULDIP CHAHAL

Date program adopted: September 1, 2016

Revised on: January 17, 2019, Oct 07, 2019, August 1,2020

Updated on October 29, 2021

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

TABLE OF CONTENTS

Part A – BACKGROUND INFORMATION

This section provides a high-level summary regarding what money laundering and terrorist financing is, and our obligations under the law. This summary relies on information provided in the Financial Transactions and Reports Analysis Centre of Canada's (FINTRAC's) *Guideline 1, Backgrounder*, and the full version of the guideline can be found on FINTRAC's website: http://www.fintrac-canafe.gc.ca/guidance-directives/overview-apercu/Guide1/1-eng.asp. Canada participates in the worldwide fight against money laundering and the financing of terrorist activities primarily through a national piece of legislation called the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (The Act) and the applicable regulations which support it. The Act's purposes are to:

- Help detect and deter money laundering and the financing of terrorist activities
- Implement reporting and other requirements on those engaged in businesses, professions and activities susceptible to being used for money laundering and terrorist financing
- Establish FINTRAC as the agency responsible for collecting, analyzing and disclosing information to assist in finding and preventing money laundering and terrorist financing in Canada and abroad.

i). What is Money Laundering?

Money laundering is the process where money and property generated by criminal activities is disguised as coming from a legitimate source.

There are three stages in the money laundering process:

- ✓ **Placement** involves placing the proceeds of crime in the financial system.
- ✓ **Layering** involves converting the proceeds of crime into another form and creating complex layers of financial transactions to hinder the audit trail and disguise the source and ownership of funds.
- ✓ **Integration** involves placing the laundered proceeds back in the economy to create the perception of legitimacy.

Money laundering starts with the proceeds of crime from a predicate offence. A predicate offence includes but is not limited to tax evasion, illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation, and copyright infringement. A money laundering offence can include property or proceeds derived from illegal activities that took place outside Canada.

Methods of Money Laundering

There are as many methods to launder money as the imagination allows, and the methods used are becoming increasingly sophisticated and complicated as technology advances. Often money is laundered using nominees such as family members, friends or associates who are trusted within the community, and who will not attract attention, to help conceal the source and ownership of funds and to conduct transactions. Another common method is structuring, or smurfing where multiple inconspicuous individuals deposit funds into a central account, usually in amounts less than thresholds for reporting. Examples of flags to be aware of and transactions which could be connected to money laundering are provided in section v) below.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

ii). What is Terrorist Financing?

Under Canadian law, terrorist activity financing is when you knowingly collect or provide property, such as funds, either directly or indirectly, to terrorists. The main objective of terrorist activity is to intimidate a population or compel a government to do something.

Terrorists need financial support to carry out terrorist activities and achieve their goals. Many of the techniques used to perform money laundering are also used within terrorist financing, including, but not limited to obscuring the direction of funds and the use of third parties. They need to disguise their money as coming from another source, and put it into a form that cannot be easily traced so that it is useable.

Methods of Terrorist Financing

There are two primary sources of financing for terrorist activities. The first involves getting financial support from countries, organizations or individuals. The other involves revenue-generating activities of terrorist groups that may include legitimate and criminal activity. Terrorist groups may use smuggling, fraud, theft, robbery and narcotics trafficking to generate funds.

Financing for terrorist groups may also include legitimately earned income, which might include collection of membership dues and subscriptions, sale of publications, speaking tours, cultural and social events, as well as solicitation and appeals within the community. This fundraising might be in the name of organizations with charitable or relief status, so that donors are led to believe they are giving to a legitimate good cause.

The methods used by terrorist groups to generate funds from illegal sources are often very similar to those used by “traditional” criminal organizations. For this reason, transactions related to terrorist financing may look a lot like those related to money laundering. Therefore, strong, comprehensive anti-money laundering regimes are key to also tracking terrorists' financial activities.

iii). Our Responsibilities

All insurance agents or agencies in Canada are reporting entities under the Act and are required to:

- Establish a compliance program to ensure compliance with their reporting, record-keeping and client identification requirements
- Follow rules regarding client identification and keep certain records regarding specific transactions
- Report to FINTRAC suspicious transactions, large cash transactions and information regarding terrorist property

The elements of a compliance program required under the Act are as follows:

- Appointment of a compliance officer
- The development and application of written compliance policies and procedures
- The assessment and documentation of money laundering and terrorist financing risks for the business, along with steps to mitigate those risks
- An ongoing training plan, if the agent or agency has employees or others authorized to act on the agent or agency’s behalf
- A plan to review the compliance policies and procedures and your risk assessment, and a plan to test their effectiveness at least every two years

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

iv). Penalties for Non-Compliance

FINTRAC can issue an Administrative Monetary Penalty (AMP) to reporting entities that are not compliant with Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

Violations are classified by the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* as minor, serious or very serious and carry the following range of penalties:

- Minor violation: from $1 to $1,000 per violation
- Serious violation: from $1 to $100,000 per violation
- Very serious violation: from $1 to $100,000 per violation for an individual, and from $1 to $500,000 per violation for an entity (e.g. corporation)

The limits above apply to each violation, and multiple violations can result in a total amount that exceeds these limits. A list of violations is available on the Justice Canada website.

FINTRAC may disclose cases of non-compliance to law enforcement when there is extensive non-compliance or little expectation of immediate or future compliance.

Criminal penalties may include the following:

- Failure to report suspicious transactions: up to $2 million and/or five years imprisonment.
- Failure to report a large cash transaction or an electronic funds transfer: up to $500,000 for the first offence, $1 million for subsequent offences.
- Failure to meet record keeping requirements: up to $500,000 and/or five years imprisonment.
- Failure to provide assistance or provide information during compliance examination: up to $500,000 and/or five years imprisonment.
- Disclosing the fact that a suspicious transaction report was made, or disclosing the contents of such a report, with the intent to prejudice a criminal investigation: up to two years imprisonment.

Penalties for failure to report do not apply to employees who report suspicious transactions to their superior.

v). Indicators of Suspicious Transactions or Potential High-Risk Clients

The following are some samples of some general and industry-specific indicators that might lead you to have reasonable grounds to suspect that a transaction is related to a money laundering or terrorist activity financing offence. The presence of one or more of these factors does not indicate the transaction is suspicious and reportable to FINTRAC, but that a deeper look should be taken.

General indicators

The following are a few examples of general indicators that might lead us to suspect that a transaction is related to a money laundering or terrorist activity financing offence. It will not be just one of these factors alone, but a combination of several factors in conjunction with what is normal and reasonable in the circumstances of the transaction or attempted transaction.

- ✓ Client admits to or makes statements about involvement in criminal activities
- ✓ Client produces seemingly false documentation that appears to be counterfeited, altered or inaccurate

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- ✓ Client does not want correspondence sent to home address
- ✓ Client appears to have accounts with several financial institutions in one area for no apparent reason
- ✓ Client repeatedly uses an address but frequently changes the name involved
- ✓ Client is accompanied and watched
- ✓ Client shows uncommon curiosity about internal controls and systems
- ✓ Client presents confusing details about the transaction
- ✓ Client makes inquiries that would indicate a desire to avoid reporting
- ✓ Client is involved in unusual activity for that individual or business
- ✓ Client insists that a transaction be done quickly
- ✓ Client seems very conversant with money laundering or terrorist activity financing issues
- ✓ Client refuses to produce personal identification documents
- ✓ Client frequently travels to a high-risk country

Industry specific examples

- ✓ Client wants to use cash for a large transaction
- ✓ Client proposes to purchase an insurance product using a cheque drawn on an account other than his or her personal account
- ✓ Client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment
- ✓ Client who has other small policies or transactions based on a regular payment structure makes a sudden request to purchase a substantial policy with a lump sum payment
- ✓ Client conducts a transaction that results in a conspicuous increase in investment contributions
- ✓ Scale of investment in insurance products is inconsistent with the client's economic profile
- ✓ Unanticipated/inconsistent modification of client's contractual conditions, including significant or regular premium top-ups
- ✓ Unforeseen deposit of funds or abrupt withdrawal of funds
- ✓ Involvement of one or more third parties in paying the premiums or in any other matters involving the policy
- ✓ Overpayment of a policy premium with a subsequent request to refund the surplus to a third party
- ✓ Funds used to pay policy premiums or deposits originate from different sources
- ✓ Use of life insurance product in a way that resembles use of a bank account, namely making additional premium payments and frequent partial redemptions
- ✓ Client cancels investment or insurance soon after purchase
- ✓ Early redemption takes place in the absence of a reasonable explanation or in a significantly uneconomic manner
- ✓ Client shows more interest in the cancellation or surrender of an insurance contract than in the long-term results of investments or the costs associated with termination of the contract
- ✓ Client makes payments with small denomination notes, uncommonly wrapped, with postal money orders or with similar means of payment
- ✓ The duration of the life insurance contract is less than three years
- ✓ The first (or single) premium is paid from a bank account outside the country
- ✓ Client accepts very unfavorable conditions unrelated to his or her health or age
- ✓ Transaction involves use & payment of performance bond resulting in cross-border payment
- ✓ Repeated and unexplained changes in beneficiary
- ✓ Relationship between the policy holder and the beneficiary is not clearly established

Additional examples can be found on FINTRAC's website in Section 8.5: http://www.fintrac.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.asp#s8-5.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

PART B – APPOINTMENT OF A COMPLIANCE OFFICER

The compliance officer is responsible for:

- The implementation, monitoring and updating of the compliance program which includes:
  - Policies and procedures for reporting, record keeping, client identification, risk assessment and risk mitigation
  - Risk-based approach
  - Training
  - Program evaluation

- Making necessary reports to FINTRAC (suspicious transactions, large cash transaction, terrorist property reports)

- Reporting on a regular basis to the board of directors/senior management/owner

The compliance officer:

- Should have the authority and the resources necessary to discharge their responsibilities effectively
- Should have a thorough understanding of AML obligations and of the practice and the client base to be able to identify risks for the practice
- May delegate certain duties to other employees however the compliance officer retains responsibility for the implementation and ongoing execution of the compliance regime.

The person below has been appointed to the position of compliance officer:

NAME: Kuldip Chahal _____

POSITION: COMPLIANCE OFFICER _____

Date _____

Appointment approved by:

_____ _____

Principal Date

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

PART C – POLICIES AND PROCEDURES

Section 1. Suspicious Transactions and Reporting Guidelines

As of January, 2019 FINTRAC, published new suspicious transaction guidance including:

1. What is a suspicious transaction report? – replaces Guideline 2: Suspicious transactions

2. Reporting suspicious transactions to FINRAC – replaces Guideline 3A: Submitting suspicious transaction reports to FINTRAC electronically and Guideline 3B: Submitting suspicious transaction reports to FINTRAC by paper

3. Sector specific "Money laundering and terrorist financing indicators

– All references to financial transactions should include ATTEMPTED or COMPLETED

The policies and procedures below provide the roles and responsibilities and information for identifying reportable transactions and reporting to FINTRAC, record keeping, record retention, ascertaining identity, risk-based approach, and training program.

1.1. What is a suspicious transaction report? January 2019

This guidance on suspicious transactions is applicable to reporting entities (REs) and individuals employed by reporting entities 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 all other suspicious transaction reporting (STR) guidance, including:

- Reporting suspicious transactions to FINTRAC; and
- Money laundering (ML) and terrorist financing (TF) indicators (ML/TF indicators)

****Note:** All references to financial transactions should be read to include **attempted** or **completed** financial transactions.

This document serves to answer the following questions:

- *What is an STR and why are they vital to FINTRAC and to Canada's anti-money laundering and anti-terrorist financing regime?*
- *How do you identify a suspicious transaction? What is "reasonable grounds to suspect" and when do you submit an STR to FINTRAC?*
- *What are reasonable grounds to suspect and when do you submit an STR to FINTRAC?*
- *How does FINTRAC assess an RE's compliance with its obligation to submit STRs?*
- *How can a RE assess its own compliance with its obligations to submit STRs?*

- ***What is an STR and why are they vital to FINTRAC and to Canada's anti-money laundering and anti-terrorist financing regime?***

FINTRAC operates within the legislative authority of the PCMLTFA and associated Regulations. Its mandate is to detect, prevent and deter instances of ML/TF activities.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

FINTRAC requires that certain individuals and entities implement specific measures as a part of their compliance program and submit various types of reports to FINTRAC. FINTRAC uses these reports to assess and analyze financial transactions to create a picture that serves to uncover financial relationships and networks that will:

- assist in criminal investigations and prosecutions of offences related to ML/TF, as well as threats to the security of Canada;
- detect trends and patterns related to ML/TF risks;
- uncover vulnerabilities to Canada's financial system; and
- enhance public awareness of ML/TF matters.

One of the most valuable types of reports in relation to the analysis and production of financial intelligence is the STR. You must submit an STR to FINTRAC where you have determined that you have reasonable grounds to suspect that a financial transaction is related to the commission or attempted commission of an ML/TF offence. This means that you have reasonable grounds to suspect that the financial transaction(s) is assisting a terrorist or terrorist group or both, or in the case of ML, is being used to convert the proceeds of crime into the appearance of a legitimate activity.

STRs must be detailed and of high quality, as they provide invaluable financial intelligence for FINTRAC's analysis such as individuals or entities' names, accounts, locations and relationships that may ultimately be disclosed to law enforcement, intelligence agencies, and/or other disclosure recipients. They also provide context and make connections that disclosure recipients may not otherwise have known about.

FINTRAC reviews and assesses every STR within days of its receipt. When warranted, such as in the case of STRs related to threats to the security of Canada, FINTRAC has disclosed financial intelligence to disclosure recipients within 24 hours by expediting the analysis and the assessment to determine if the prescribed thresholds to disclose are reached. As such, STRs are critical to FINTRAC's analytical function and to its ability to detect, prevent and deter ML/TF. Consequently, a failure to report an STR may have a direct impact on FINTRAC's capacity to carry out its mandate, including FINTRACs ability to aid in the protection of Canada's national security, therefore impeding the achievement of the objective of the PCMLTFA and associated Regulations.

For more information on ML or TF, see FINTRAC's Guideline 1: Backgrounder.

❖ ***How do you identify a suspicious transaction?***

Most often, it is a combination of facts, context and ML/TF indicators that will lead to the determination of whether you have reasonable grounds to suspect that a transaction is related to the commission or attempted commission of an ML/TF offence.

What is a fact?

A fact, in regards to completing an STR, is an actual event, action, occurrence or element that exists or is known to have happened or existed. It cannot be an opinion. For example, facts surrounding a financial transaction could include the date, time, location, amount or type of transaction or could include the account details, particular business lines, or the client's financial history. It could also include information about your client should the information be known to be true (e.g. that they are a convicted felon, or that they are the subject of a production order).

What is context?

Understanding the context of a financial transaction(s) that may be observed or acquired through:

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- a general awareness of the events occurring in your client's business environment or community;
- your knowledge of the typical financial activities found within your business;
- regular know your client (KYC) activities (e.g. who they are, their occupation or business, how they generate their wealth, typical or expected transactional behavior, etc.);
- the information obtained through the application of your risk-based approach; and
- the background and/or behavior/actions of a client.

This type of information is essential in determining what is suspicious. Context in regards to completing an STR is clarifying a set of circumstances or providing an explanation of a situation or financial transaction that can be understood and assessed.

If the context surrounding a particular transaction is unusual or suspicious, it could lead you to assess your client's current and past financial transactions.

A financial transaction may not appear suspicious in and of itself. However, additional context about the associated individual or their actions may create suspicion.

Your suspicion of ML/TF will most likely materialize out of an assessment of multiple elements that, when viewed together, will either inform or negate suspicion of ML/TF.

For example, suspicion may materialize through:

- An individual:
  - asks several questions about their reporting obligations (fact)
  - wants to know how they can avoid their transaction being reported to FINTRAC (context)
  - structures their amounts to avoid client identification or reporting thresholds (context)
  - keeps changing their explanation for conducting a transaction or knows few details about its purpose (context)

- An individual making a deposit to a personal account, where that individual:
  - has a low salary (context) and has deposited an irregularly large amount of money (fact)?
  - keeps changing their explanation for the deposit or cannot / will not provide an explanation (context)
  - exhibits nervous behavior (context)

- Transactions to a business account with the following additional elements:
  - deposits to the account are made by numerous parties that are not signing authorities or employees (fact)
  - the account activity involves wire transfers in and out of the country (fact), which does not fit the expected pattern of that business (context)
  - multiple deposits are made to the account by third parties (fact)

What is an ML/TF indicator?

ML/TF indicators are potential red flags that could initiate suspicion or indicate that something may be unusual without a reasonable explanation. Red flags typically stem from one or more factual characteristics, behaviors, patterns or other contextual factors that identify irregularities related to financial transactions. These often-present inconsistencies with what is expected or considered normal based on what you know about your client.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

FINTRAC has published ML/TF indicators for each sector that were developed 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 indicator may not appear suspicious. However, observing an indicator(s) could lead you to assess the transaction(s) to determine whetherthere are further facts, contextual elements or additional ML/TF indicators that might require the submission of an STR.

Criminal organizations often combine various methods in novel ways in order to avoid the detection of ML/TF. ML/TF indicators can prompt your suspicion but it is the assessment of facts, context and ML/TF indicators that can help you determine if 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 may also be used to explain or articulate the reasons for your reasonable grounds to suspect in an STR.

- **What are reasonable grounds to suspect and when do you submit an STR to FINTRAC?**

Reasonable grounds to suspect is a step above simple suspicion and is a conclusion you reach based on an assessment of facts, context, and ML/TF indicators associated with the financial transaction. Your suspicion must be reasonable, meaning, for example, that it cannot be biased or prejudiced.

It is through an assessment of information that you are able to demonstrate and articulate your suspicion of ML/TF in such a way that another individual reviewing the same material with similar knowledge, experience, or training would likely reach the same conclusion.

Reaching reasonable grounds to suspect means that you consider all the facts, context and ML/TF indicators related to a financial transaction and, after having reviewed this information, you conclude that there are reasonable grounds to suspect that this particular financial transaction is related to ML/TF. It is possible that you have one piece of information that was so compelling that it led you to start an assessment or submit an STR to FINTRAC.

Once you determine that there are reasonable grounds to suspect that a transaction is related to the commission of attempted commission of an ML/TF offence, you must submit an STR to FINTRAC.

Understanding the differences between the thresholds can help to clarify what reasonable grounds to suspect means for your organization and how it can be operationalized within your compliance program.

- **How does FINTRAC assess an RE's compliance in their determination of reasonable grounds to suspect?**

FINTRAC conducts various activities to ensure that STRs are properly completed and submitted, including an evaluation of their quality, timing and volume. If you are reporting multiple suspicious financial transactions involving the same client(s) or account(s), you would periodically re-assess their level of risk and apply the appropriate measures determined by your risk-based approach. This assessment could include a review of transactional records to ensure that you are keeping a copy of the STR as required by the PCMLTFA and associated Regulations.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

FINTRAC can use various assessment methods to ensure that you are detecting and submitting complete STRs in a timely manner. During an assessment, FINTRAC expects that you will be able to:

- confirm that you have an ongoing monitoring process that enables you to detect, assess and, when applicable, report suspicious transactions;
- explain how your process for detecting and assessing suspicious transactions is reasonable, effective, & consistent with your risk assessment across all business lines;
- demonstrate how you identify relevant transactions; and
- show your record keeping and decision-making processes.

There may be times where you initially assessed transactions as suspicious, but as a result of your re-assessment, later negated the suspicions and determined the transactions reasonable. As a best practice, you may want to document the rationale and keep a record as to why the suspicion was negated. Keeping a record of these decisions is not required but may be helpful to you in the context of a FINTRAC assessment.

You can rely on ML/TF indicators, open source, media reporting or FINTRAC's operational briefs and alerts to help you identify suspicious financial transactions and determine reasonable grounds to suspect.

It is important to remember that your STR program is linked to the overall effectiveness of your compliance program. A timely and well-prepared STR could be crucial to Canada's anti-money laundering and anti-terrorist financing regime. To ensure that you have submitted an STR in a timely manner, FINTRAC will look at the date that you detected a fact that led you to reach reasonable grounds to suspect that an ML/TF offence had been committed (or attempted). FINTRAC will also look at your overall STR program to evaluate its effectiveness in terms of identifying, assessing and submitting STRs as per your policies and procedures.

You may decide to expedite the submission of STRs in certain situations involving time-sensitive information and threats to national security, such as suspected terrorist financing.

❖ **How can a RE assess its own compliance with its obligations to submit STRs?**

Part of your regulatory obligations is the requirement to assess the effectiveness of your compliance program as a part of your two-year review. In support of this, below are some examples you may wish to consider for your own assessment:

a. You may decide to assess STRs with similar scenarios to ensure that you are applying consistency. For example, if you found certain ML/TF indicators through your assessment that support your suspicions of ML/TF, you should be aware when the same ML/TF indicators appear elsewhere to ensure that you are not missing potential STRs that should be or should have been submitted to FINTRAC. This approach can help you build consistency within your organization.
b. If you submitted an STR to FINTRAC in respect of a financial transaction(s) conducted by a client, you should continue to submit STRs as long as the suspicions of ML/TF continue. That being said, you should periodically re-assess the information to evaluate your grounds for suspicion. How often you perform this assessment can be documented as part of your policies and procedures. For instructions on submitting multiple STRs on the same client, refer to Reporting suspicious transactions to FINTRAC.
c. You can work within your industry to identify how others are reaching the reasonable grounds to suspect threshold and to establish common baselines for what could be

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

considered unusual or suspicious. Please consult FINTRAC's operational briefs and alerts for more information on ML/TF that has been observed within certain sectors or relating to specific criminality (e.g. human trafficking, fentanyl, etc.).

d. Reasonable grounds to suspect means that you can explain the reasons for your suspicion in such a way that another individual with similar knowledge, experience and training would, based on the same information, likely reach the same conclusion. Applying this logic can direct your assessment of financial transactions that may fit some of the ML/TF indicators identified by FINTRAC. This will also help you determine if there are financial transactions that should be considered for further assessment and potential reporting to FINTRAC.
e. To assess your timing for submitting an STR, you may wish to conduct a sample review to ensure that your STRs were sent in a timely manner. You can also assess the relevant aspects of your STRs (facts, context and ML/TF indicators) and determine when they became known to ensure that you are reporting them from the date you reached the reasonable grounds to suspect threshold.
f. To assess the quality of your STRs, it is important that you consider the consistency and integrity of your KYC information and provide all relevant information that led to the determination of the reasonable grounds to suspect threshold.
g. STRs have significantly fewer mandatory fields than other FINTRAC reports. This is intended to encourage reporting even in situations where you may not have information because the client did not provide any or where asking for details might 'tip off' the individual to your suspicions. Double-checking the quality of your STRs before submitting them is important because FINTRAC cannot automatically reject reports that have missing information, unlike other report types. However, FINTRAC expects that if you can access the information in your institution, it must be reported.

1.2. Reporting suspicious transactions to FINTRAC – January 2019

Suspicious transaction reporting requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations are applicable to all reporting entity sectors.

It is recommended that this guidance be read in conjunction with other STR guidance, including:

- What is a suspicious transaction report?
- Money laundering (ML) and terrorist financing (TF) indicators (ML/TF indicators)

****Note:** All references to financial transactions should be read to include **attempted** or **completed** financial transactions.

This guidance provides information on the following topics:

- When must a suspicious transaction be reported?
- Service provider agreements
- How to submit STRs
- Review and validation of reports by FINTRAC
- Completing the STR form
- Field completion instructions

Life insurance companies, brokers and agents

If you are a life insurance company and you have foreign subsidiaries or foreign branches, the suspicious transaction reporting requirement does not apply to the operations of these subsidiaries or branches outside Canada.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- **When must a suspicious transaction be reported?**

Pursuant to section 9(2) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations, "the report shall be sent to the Centre within 30 days after the day on which the person or entity or any of their employees or officers detects a fact respecting a financial transaction or an attempted financial transaction that constitutes reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering offence or a terrorist financing offence." In other words, an STR must be submitted to FINTRAC when you detect a fact that leads you to determine that you have **reasonable grounds to suspect** that a transaction is related to the commission or attempted commission of a money laundering or terrorist financing offence.

You must submit an STR to FINTRAC "As soon as practicable". Unlike all other reporting obligations, there is no monetary threshold associated with the reporting of a suspicious transaction. STRs are unique under the Canadian anti-money laundering and anti-terrorist financing (AML/ATF) regime as they may also contain transactions that must be submitted to FINTRAC in other types of reports. For example, if a completed transaction reported in an STR involved the receipt of cash from a client of 10,000 Canadian Dollars (CAD) or more, you would also be required to report this transaction to FINTRAC in a large cash transaction report.

- **Service provider agreements**

A service provider can submit and correct STRs on your behalf. However, as the reporting entity, you are ultimately responsible for meeting your obligations under the PCMLTFA and associated Regulations, even if a service provider is reporting on your behalf. This legal responsibility cannot be delegated.

- **How to submit STRs**

If you have a computer and an internet connection, you must submit STRs to FINTRAC electronically. You must submit by paper if you do not have the technological capacity to send an STR electronically.

There are two options for electronic reporting that provide for secure encrypted transmission that ensures your data's confidentiality and integrity. These two electronic reporting options are listed below.

- FINTRAC's secure website - F2R
- Batch file transfer

For more information about FINTRAC's electronic reporting system enrolment, see our electronic reporting page.

F2R reporting
F2R is a secure application accessed through the internet that allows you to manually submit individual reports, as well as correct those reports if needed. F2R is geared towards reporting entities with lower reporting volumes. **To report STRs electronically**, you must be enrolled and logged in to the F2R system. For more information on F2R reporting, see the following documents:

- F2R reporting: for instructions on how you can enroll in F2R and the browser requirements; and

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- F2R Electronic Reporting User Guide: for instructions on how to use the application.

Batch reporting
Batch reporting is a secure process that allows for the submission and correction of multiple reports (up to 10,000) in 'Batch files' that are formatted according to FINTRAC's specifications. To use the Batch reporting system, FINTRAC will provide you with Batch transmission software but you will also need to enroll in F2R and apply for a public key infrastructure (PKI) certificate. For more information on Batch reporting, see the following links and documents.

- How can I use Batch reporting? for instructions on how you can enroll in F2R and apply for a PKI certificate.
- Batch transmission guide: to assist you with installing and configuring the Batch transmission software and to instruct you in how to transmit Batch files to FINTRAC.
- Batch documentation: to assist you with how to create, submit and correct Batch files.

Paper reporting
FINTRAC's STR paper reporting form can be printed from the reporting forms webpage or you can request a form to be faxed or mailed to you by calling FINTRAC at 1-866-346-8722.

To ensure that the information provided is legible and to facilitate data entry, it would be preferable if the free-text areas of the STR (Parts G and H) were completed using word-processing equipment. For reports completed by hand, please use black ink and CAPITAL LETTERS.

There are two ways you can send a completed paper STR form to FINTRAC:

- by fax: 1-866-226-2346; or
- by mail to the following address:

  Financial Transactions and Reports Analysis Centre of Canada
  Section A
  234 Laurier Avenue West, 24th floor
  Ottawa, ON K1P 1H7
  CANADA

There is no official acknowledgement of receipt when you send a completed paper STR form to FINTRAC. However, FINTRAC will contact you and request that you resubmit electronically if you have the capability to do so.

♦ **Review and validation of reports by FINTRAC**

FINTRAC reviews each report that is submitted to ensure that mandatory information is provided as per the PCMLTFA and associated Regulations. There are three types of validation rules that FINTRAC uses to validate reports and these rules are described below.

- Presence – is there an entry in the field?
- Format – is the entry in the correct structure?
- Content – is the correct information entered in the appropriate field?

FINTRAC validation rules identify possible reporting problems or information gaps but do not cover all scenarios. While FINTRAC conducts a review of report submissions to assess the quality of reports, you should have your own proactive quality assurance practices independent of FINTRAC's review and validation of reports.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

The report validation processes for F2R and Batch are different. Each report validation process is described in more detail below.

F2R report validation
Reports submitted through F2R are immediately validated by the application. F2R will indicate where information is missing, incorrect, or improperly formatted. You **must** correct all errors for mandatory fields before you can submit a report.
You **must** correct all errors for mandatory fields before you can submit a report.

Batch report validation
Once a Batch file has been submitted, FINTRAC validates the Batch file against the validation rules. If there is an error with the structure or format of the file then you will receive a "Rejected" message and the Batch file and reports within it will not be processed any further. **You must correct and resubmit the entire Batch file.** Once you resubmit a Batch file, it is revalidated against all validation rules.

If there is a potential issue in a reporting field then you may also receive a "Warning" message. If you receive a "Warning" message, the report has been accepted by FINTRAC but you should review the information submitted for accuracy and completeness.

Once your Batch file has been accepted and validated, FINTRAC will send you a Batch "Acknowledgement" message that will include the validation rule number(s) for any report(s) that require further action and any warning messages.

See FINTRAC's Standard Batch Reporting Instructions and Specifications for more information.

- **Completing the STR form**

FINTRAC's expectations for completing an STR

It is your responsibility to ensure that the information provided in an STR is complete and accurate. Your policies and procedures must include details on the process for how you identify, assess and submit STRs to FINTRAC. It is possible that your organization has an automated or triggering system that detects unusual or suspicious transactions that would require assessment by a person to determine if you must submit an STR. A person with the appropriate knowledge and training is expected to be able to determine whether a transaction is related to the commission or attempted commission of an ML/TF offence. It is also important to note that the value of the transaction is not always the most important aspect of an STR. Training employees to perform this function is considered to be part of your compliance program obligations.

Please note, an employee of a reporting entity can be considered a 'reporting entity' and report a completed or attempted suspicious transaction to FINTRAC when:

- they have reasonable grounds to suspect that a transaction is related to the commission or attempted commission of an ML/TF offence; and
- their employer did not or will not report.

This stipulation is in place to cover the rare instances where an individual suspect that the thresholdto report has been reached and their employer did not or will not send an STR. No individual or entity will be prosecuted for sending an STR in good faith or for providing FINTRAC with informationabout suspicions of money laundering or terrorist financing. To submit an STR in this scenario, you

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

may use the paper report form. For more information, please see field completion instructions to submit STRs by paper.

It is important to FINTRAC's analysis process and disclosure recipients that the STRs you submit are comprehensive and of high quality. In Part G or H of the STR, it is important to **avoid jargon or non-public references**, such as terms and acronyms that are specific to your organization. Please consider an outside reader and use simple, clear and concise language.

A variety of information is often collected as part of an assessment to determine if you are required to submit an STR and this information is valuable to include in your report to FINTRAC.
A well-completed STR should consider the following questions.

1. **Who** are the parties to the transaction?

    - List the **conductor, beneficiary and holders** of all accounts involved in the transaction.
    - Take **reasonable measures** to identify the conductor of the transaction. This means that you are expected to ask the client for this information unless you think doing so will tip them off to your suspicion.
    - Provide **identifying information** on the parties involved in the transaction. This could include the information you recorded to identify the conductor, as well as any information you have on the other parties to the transaction or its recipients.
    - **List owners, directors, officers and those with signing authority, when possible.** If the transaction involves a business, you could include information on the ownership, control and structure of the business in the STR.
    - Provide **clear information about each individual or entity's role** in each of the financial transactions described. It is important to know who is sending and receiving the funds and this may be relevant in Part G of the STR.
    - **Explain the relationships among the individuals or entities (if known).** This is very helpful to FINTRAC when trying to establish networks of individuals or entities suspected of being involved in the commission or attempted commission of an ML/TF offence.

2. **When** was the transaction(s) completed/attempted? If it was not completed, why not?
    - Provide the **facts, context and ML/TF indicators** regarding the transaction.

3. **What** are the financial instruments or mechanisms used to conduct the transaction?

4. **Where** did this transaction take place?

5. **Why** the transaction(s) or attempted transaction(s) are related to the commission or attempted commission of an ML/TF offence?
    - State the ML/TF indicators used to support your suspicion.
    - State the **suspected** criminal offence related to ML/TF, if known.

6. **How** did the transaction take place?

Once you have reached reasonable grounds to suspect, you must keep reporting as long as the suspicion remains. You are expected to periodically re-assess the client to verify that the level of suspicion has not changed. This process may be part of your documented risk-based approach or ongoing monitoring. If you continue to report STRs(s) on the same person or entity, you can reference a previous STR in Part G by:

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- entering the FINTRAC STR number and date of submission;
- providing the reasonable grounds to suspect (facts, context and ML/TF indicators) that were included in the first STR submission; and
- by providing any new additional information.

If you are reporting STRs because the assessment has changed due to new facts, context and/or ML/TF indicators, you are expected to provide them. For example, through the course of your assessment, you may have identified new ML/TF indicators or new parties transacting with your client. You may choose to include that information under a separate heading in Part G so that it is properly labeled as new information.

You must keep a copy of all STRs submitted to FINTRAC. For more information on your record keeping obligations related to STRs, see your sector specific record keeping guidance.

STR submission limitations

Each STR must include at least one transaction and may include up to 99 transactions as long as all the transactions:

- have the same transaction status (e.g., all completed transactions or all attempted transactions); and
- took place at the same location.

For example, someone brings a money order for $6,000 CAD and successfully sends an electronic funds transfer for $6,000 CAD (**first completed transaction**). Later that day, the same person returns to the same location and brings $5,000 CAD cash and receives a money order (**second completed transaction**). In this case, if there are reasonable grounds to suspect that the two completed transactions, conducted at the same location, are related to the commission or attempted commission of an ML/TF offence, you should provide the transaction details for the two transactions in the same STR. **While the transactions may be referenced in Part G as part of the facts, context and/or ML/TF indicators, the transaction details themselves must be entered in Parts B1 through F.**

In a situation where, related suspicious transactions took place at **different locations**, an STR must be submitted **for each location** and only detail the transactions that occurred at that specific location. In addition, all transactions should have the same status as either completed or attempted to be included in a single report.

If you have more than 99 transactions to report at one time, you must submit the additional transaction(s) in a separate STR. You cannot insert a spreadsheet or include the additional transactions in Part G of the STR. If the information is available, you can reference related STRs in Part G by entering the FINTRAC STR number and date of submission.

Common STR deficiencies to avoid

The following are examples of deficiencies that FINTRAC has identified through its assessments and other compliance activities. FINTRAC is sharing these examples to illustrate common errors that you can avoid.

1. **Using a higher threshold as your basis for reporting:** You are required to submit an STR when you have determined that there are **reasonable grounds to suspect** that a transaction is related to the commission or attempted commission of an ML/TF offence. In some cases, it is possible that you have determined that there are **reasonable grounds to**

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

believe that the transaction is related to the commission or attempted commission of an ML/TF offence. In those cases, you should still submit an STR. However, it is important to note that you do not need to reach the threshold of reasonable grounds to believe in order to submit an STR.

2. **Failing to list all the transactions and accounts relevant to your suspicion in Parts B through F:** You are required to report all the transactions and accounts in Parts B through F that led to your determination that there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence. Providing a summary of the transactions in Part G is not enough.

3. **Not listing or naming all parties to the transactions when the information is available:** All parties to the transaction must be listed, including third parties. You should also specify whether the parties are known or unknown. This has been observed in transactions involving multiple parties such as wire transfers. For example, if you are reporting a wire transfer, you should include any information you have regarding both the ordering client and beneficiary. This could include (but is not limited to) their names, their account number and institution, their relationship, and any known identifiers. FINTRAC acknowledges that this information may not always be at your disposal, but when you know it, it should be provided.

4. **Part G does not elaborate on your grounds for suspicion or link them to the transactions reported in Parts B through F:** You are required to articulate the reasons for your determination that there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence in an STR. This includes providing all of the relevant facts, context and ML/TF indicators related to the transactions reported in Parts B through F that support your suspicion in Part G. This deficiency has been observed when a reporting entity does not articulate the reasons for their suspicion or does not explain how or why certain information is relevant to their suspicion.

- **Field completion instructions**

****Note:** Unless otherwise stated, this section details specific instructions that **apply to both electronic and paper reporting**.

Parts of a suspicious transaction report

STRs contain eight specific parts:

- **Part A: Information about where the transaction took place**

In Part A of the STR, you must provide information about you as the reporting entity, and about the physical location where the completed or attempted suspicious transaction took place.

When completing Part A it is important to note that:

- **Reporting entity's full name** is your entity's full legal name. Even if you have entered into a contractual relationship with another entity to conduct transactions on your behalf, it is your name that **must** be entered into this field.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- **Reporting entity number** is the number that was assigned to you when you enrolled in F2R.
- **Reporting entity location number** is the location number where the transaction took place or was attempted. If you have multiple locations, your F2R administrator is responsible for adding the other locations, as well as maintaining the location information.
- **Reporting entity report reference number** is a unique internal reference number generated by your entity. The recording of the internal reference number on the STR may help you to quickly identify the report if required to at a later date.
- **Activity Sector** is the type of business and/or activities you undertake.

- **Part B1: Information about how the transaction was initiated**
-

In Part B1 of the STR, you must provide the date of the transaction, the transaction amount, the detail of the funds involved in initiating the transaction, how the transaction was conducted, as well as information on any other institution, entity or individual that was involved in the transaction.

When completing Part B1 it is important to note that:

- the date of transaction is the date that the transaction occurred. Whereas, the date of posting is the date on which the funds from the transaction are received in an account; and
- you must provide (if applicable) the name of any other person or entity or the name and number of the other institution **involved in the initiation of** the transaction.

If you need to report more than one transaction in an STR, a separate Part B1 will have to be completed for each transaction.

- **Part B2: Information about how the transaction was completed**

In Part B2 of the STR, you must detail:

- how the funds were used in the completed transaction or how they were going to be used in an attempted transaction; and
- whether the individual who conducted or attempted the suspicious transaction did so on anyone else's behalf.

The funds in a transaction may have been used in several ways, therefore resulting in more than one disposition having to be detailed in your STR. For example, your client may initiate a transaction in cash, then use some of the funds to send an electronic funds transfer (disposition 1), order a bank draft (disposition 2), and deposit the remaining funds (disposition 3). If there is more than one disposition, you will need to complete a separate Part B2 for each disposition.

- **Part C: Account information, if the transaction involved an account**

In Part C of the STR, you must provide the account details for **each disposition** that involved an account (completed transaction) or was going to involve an account (attempted transaction), if applicable. For example, if the related disposition was a "Deposit', this part is required.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

• **Part D: Information about the individual conducting the transaction**

In Part D of the STR, you must provide information about the individual who completed or attempted to complete the transaction.
If more than one transaction is reported in an STR, a **separate Part D** will have to be completed **for each transaction.**

• **Part E: Information about the entity on whose behalf the transaction was conducted**

In Part E of the STR, if applicable, you must provide information about the entity on whose behalf the transaction was conducted or attempted.
Part E needs to be completed if you indicated in Part B2 that the transaction was conducted "On behalf of an entity."
A separate Part E must be completed for **each** disposition that was conducted or attempted on behalf of an entity.

• **Part F: Information about the individual on whose behalf the transaction was conducted**

In Part F of the STR, if applicable, you must provide information about the individual on whose behalf the transaction was conducted or attempted.
Part F must be completed if you indicated in Part B2 that the transaction was conducted "On behalf of another individual."
A separate Part F must be completed for each disposition that was conducted or attempted on behalf of another individual.

• **Part G: Description of suspicious transaction and any facts or context associated with the suspicion**

This section is the narrative that explains your grounds for suspicion and should include the results of your assessment of facts, context and ML/TF indicators that led to your decision to submit an STR to FINTRAC. The narrative should include the explanation of this assessment and should not assume that the reader will be familiar with acronyms or terminology specific to your business. Detailed and high quality STRs provide valuable and actionable intelligence for FINTRAC and this section is shared with law enforcement and intelligence agencies in FINTRAC disclosures.

The narrative provided in this section should focus on the question: "Why do you think the transaction is suspicious of ML/TF?"

The following are examples of the type of information that, when available, have been provided in STRs and have contributed greatly to FINTRAC analysis:

- any client identification information not already captured in the transaction details listed in part B, i.e., known aliases or nicknames;
- additional contact information (phone numbers, email addresses, etc.);
- details for credit card activity including details of purchases (dates, amounts, retailer (online or in-store) and details of payments (dates, amounts, conductor and source of payment);
- details for electronic transfers (such as e-mail money transfers, wire transfers) including IP addresses and sender/recipient email addresses;
- location of ATM withdrawals;
- any related STR number(s) and the date(s) previously submitted;

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- the history the client has with you;
- links made to other people, businesses and accounts;
- information on the ownership, control and structure of an entity that is not already captured in Part B, particularly for any business entities that have a complex structure;
- the intended or expected use of an account versus the activity you may have observed;
- any other information about your interactions with the client;
- the ML/TF indicators or factors that assisted in forming the basis of your suspicion;
- any information, including publicly available information and/or information from law enforcement, that made you suspect distinctly that the transaction might be related to terrorist financing, money laundering, or both;
- any details surrounding why an attempted transaction was not completed; and
- any context or clarification about the information that was reported in the structured sections (Parts B through F).

FINTRAC has been able to identify networks of suspected money launderers and terrorist financiers through pieces of information such as email addresses and secondary identifiers (nicknames) or phone numbers. This type of information may seem insignificant but can be very important to FINTRAC, as it may identify connections among individuals, entities or crimes when compared against other FINTRAC intelligence.

It is important that your narrative is consistent with the information in Parts B through F of the STR form. For example, if you are referring to specific account activity in this section the details of those accounts and transactions should be entered in the structured fields. It is also important that you do not refer to any internal files or documents since FINTRAC cannot have access to these internal files or documents for its analysis. It is also not possible to see graphics, underlined, italicized or bolded text included in the STR.

- **Part H: Description of action taken**

Describe any actions taken by you, in addition to reporting to FINTRAC, in response to the suspicious transaction.

Examples of additional actions that you may take include:

- reporting the information directly to law enforcement;
- initiating enhanced transaction monitoring;
- closing the account(s) in question or exiting the business relationship; and/or
- cancelling, reversing or rejecting the transaction.

Reporting an STR to FINTRAC does not prevent you from contacting law enforcement directly. **However, even if you do contact law enforcement directly about your suspicions of money laundering or terrorist financing, you must still submit an STR to FINTRAC**. Some STRs have included the law enforcement agency's contact information in Part H of the STR when the information was reported directly to law enforcement and this information can be helpful.

Standardized field instructions

This section includes standardized instructions for the level of effort that is required for certain fields as well as standard instructions for completing fields for identification, addresses, telephone numbers and occupation.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

1. Each field within an STR is categorized as either mandatory, mandatory if applicable, or reasonable measures.

a. Mandatory:
- Mandatory fields require you to obtain the information to complete the STR and will be marked with an asterisk (*).
- However, in the case of an **attempted transaction**, you are to take reasonable measures to obtain the information for any mandatory field.

b. Mandatory, if applicable:
- Mandatory if applicable fields must be completed if they are applicable to you or the transaction being reported. If applicable, you must provide the information if you obtained it at the time of the transaction, or if it is contained within your institution.
- These fields will be indicated with both an asterisk (*) and "(if applicable)" next to them.

c. Reasonable measures:
- For all other fields that do not have an asterisk, you must take reasonable measures to obtain the information.
- Reasonable measures can include asking for the information as long as you don't think it will tip off the person that you are submitting an STR.
- Reasonable measures also mean that you must provide the information if you obtained it at the time of the transaction, or if it is contained within your institution.

**Note: In certain circumstances a required report field may not be applicable. Do not enter "N/A" or "n/a" or substitute any other abbreviations, special characters (e.g., "x", "-"or "*") or words (e.g., unknown) in these fields. They are to be left blank.

2. Client identification

If you used the dual process method to identify an individual, you only need to provide the details of one of the identifiers. You can use your judgement to determine which identifier would be most advantageous to FINTRAC analysis. Please note that a Social Insurance Number (SIN) **must not be** reported to FINTRAC.

The record keeping requirement for the dual process method includes the source of the information, so FINTRAC expects the issuing jurisdiction and country to align with the source of the information, but would only expect, as per the validation rules, that the reporting entity include the country of issue for the dual process method.

In addition, you cannot use a provincial health card for identification purposes where it is prohibited by provincial legislation.

For more information on how to identify individuals and examples of acceptable photo identification documents, refer to FINTRAC's guidance on methods to identify individuals and confirm the existence of entities.

3. On behalf of indicator

Applies to Part B2 of an STR.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

You are required to take reasonable measures to determine if there is a third party instructing your client to conduct an activity or a transaction. Reasonable measures include asking your client if they are acting on someone else's instructions or retrieving the information that may already be contained in your records.

When determining whether an individual has conducted or attempted a suspicious transaction on anyone else's behalf, it is not about who owns or benefits from the money, or who is carrying out the transaction or activity, but rather about **who gives the instructions** to handle the money or conduct the transaction or particular activity. Refer to FINTRAC's guidance on third party determination requirements for more information including the record keeping requirements.

If you determine that a third party was instructing your client, then you must indicate if the transaction was conducted on behalf of an entity or on behalf of another individual.
When an individual is acting on behalf of their employer, the employer is considered to be the third party, unless the individual is conducting a cash deposit to the employer's business account. If there is no third party, or you were not able to determine whether there is a third party, then indicate that this part is not applicable.

4. Address fields

Applies to the following fields of an STR:

- A3* – A6* (mandatory)
- D5 – D9
- D20 – D24
- E3 – E7
- F4 – F8
- F19 – F23

The complete physical address includes the street number, street name, the city, province, and country. If there is no province or state applicable to the address, leave this field blank.

Please note that the following **are not valid addresses** and **should not** be provided:

- a post office box without a complete physical address (e.g., PO Box 333);
- a general delivery address; or
- only a suite number (e.g., Suite 256) without additional address information.

It is possible that some of the examples above may be included in Part G of the STR because they are relevant but they are not considered a valid address in terms of the client identification.
In cases where the individual or entity resides in an area where there is no street address, provide a detailed description which clearly describes the physical location. For example, in these unique cases you could enter "the third house to the right after the community center" as the street address where an individual lives.

A legal land description can be acceptable so long as the legal land description is specific enough to pinpoint the physical location of where the client lives. If the legal land description refers to an area or a parcel of land on which multiple properties are located, the legal land description would not be sufficient.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

For individuals who are transient (e.g., travelling in a recreational vehicle, temporarily working in a camp, etc.) and have no fixed address, you are required to provide the following:

- for Canadian residents, their permanent address is required, even if that is not where they are currently residing;
- for non-Canadian residents travelling in Canada for a short period of time, their foreign residential address is required; and
- for non-Canadian residents living in Canada for a longer period of time (e.g., a student), then the individual's temporary Canadian address should be provided.

5. Telephone number fields

Applies to the following fields of an STR:

- A10* - A10A
- D11
- D18 – D18A
- D25 – D25A
- E8 – E8A
- F9
- F10 – F10A
- F24 – F24A

If the telephone number is from Canada or the United States, enter the area code and local number (e.g., 999-999-9999).

If the telephone number is from outside Canada or the United States, enter the country code, city code and local number using a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight-digit local number.

6. Occupation fields

Applies to the following fields of an STR:

- D17
- F17

When entering an individual's occupation information, you must be as descriptive as possible. For example:

- If the individual is a manager, the occupation provided should reflect the area of management, such as "hotel reservations manager" or "retail clothing store manager."
- If the individual is a consultant, the occupation provided should reflect the type of consulting, such as "IT consultant" or "forestry consultant".
- If the individual is a professional, the occupation provided should reflect the type of profession, such as "petroleum engineer" or "family physician".
- If the individual is a laborer, the occupation provided should reflect the type of labor performed, such as "road construction worker" or "landscape laborer".
- If the individual is not working, the occupation provided should still be as descriptive as possible, such as "student", "unemployed" or "retired".

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

1.3 Money laundering and terrorist financing indicators - Life insurance companies, brokers and agents – January 2019

This guidance on suspicious transactions is applicable to life insurance companies, brokers or agents 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 behavior
- 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 related to transaction 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 life insurance or annuity providers
- ML/TF indicators specific to businesses who provide loans

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, behaviors, 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 assess 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 behavior 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.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

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 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 suspicious financial activity.

As a life insurance company, broker or agent, 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 a life insurance policy, the client refuses or tries to avoid providing information required, or provides information that is misleading, vague, or difficult to verify.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- The client refuses to provide information regarding the beneficial owners, or provides information that is false, conflicting, 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 information 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 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, 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 behavior

The contextual information acquired through the know your client (KYC) requirements or the behavior 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 may 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 behavior.
- 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 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.
- Client terminates life insurance policy after an initial payment 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, 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.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- The transactional activity far exceeds the projected activity at 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
- 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 life insurance policies 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.

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 different 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-based approach 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.
- Use of multiple foreign bank accounts for no apparent reason.
- Frequent and/or atypical transfers between the client's products and accounts 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.
- Accounts that receive relevant periodical payments and are inactive at other periods without a logical explanation.
- Abrupt change in account activity.

ML/TF indicators based on a typical 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.

- The client has multiple products at the same institution, atypical of what would be expected.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- 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.
- A client's transactions have no apparent business or economic purpose.
- Transaction consistent with publicly known trend in criminal activity.
- Transaction involves a suspected shell entity (an entity that does not have an economical or logical reason to exist).

Funds transferred in and out of an account on the same day or within a relatively short period of 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.

- 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.
- 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 related to transaction 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 assessing the financialtransaction 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.
- Client 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 terrorist operate/carry out attacks and/or where terrorists have a large support base (state sponsors or private citizens).

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

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 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 or nominee.

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 payments which are made to an account by non-account holders.
- Client conducts transaction while accompanied, overseen or directed by another party.
- 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 but refuses or is unable to answer questions related to the account or transactions

Indicators related to terrorist 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.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

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.
- An account opened in the name of an entity, a foundation or association, which may be linked or involved with a suspect terrorist organization.
- The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
- 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.
- 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.).

ML/TF indicators specific to life insurance

ML/TF indicators specific to life insurance or annuity providers

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 if you provide life insurance or annuities as your main occupation or as one of the many services that you offer. Below are some examples of sector specific ML/TF indicators that you should consider as part of your STR program.

- Client wants to use cash for a large transaction.
- Client proposes to purchase an insurance product using a cheque drawn on an account other than his or her personal account.
- Client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment.
- Client who has other small policies or transactions based on a regular payment structure makes a sudden request to purchase a substantial policy with a lump sum payment.
- Client conducts a transaction that results in a conspicuous increase in investment contributions.
- Scale of investment in insurance products is inconsistent with the client's economic profile.
- Unanticipated and inconsistent modification of client's contractual conditions, including significant or regular premium top-ups.
- Unforeseen deposit of funds or abrupt withdrawal of funds.
- Involvement of one or more third parties in paying the premiums or in any other matters involving the policy.
- Overpayment of a policy premium with a subsequent request to refund the surplus to a third party.
- Funds used to pay policy premiums or deposits originate from different sources.
- Use of life insurance product in a way that resembles use of a bank account, namely making additional premium payments and frequent partial redemptions.
- Client cancels investment or insurance soon after purchase.
- Early redemption takes place in the absence of a reasonable explanation or in a significantly uneconomic manner.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- Client shows more interest in the cancellation or surrender of an insurance contract than in the long-term results of investments or the costs associated with termination of the contract.
- Client makes payments with small denomination notes, uncommonly wrapped, with postal money orders or with similar means of payment.
- Changing the duration of the life insurance contract from the original purpose and intended use.
- The first (or single) premium is paid from a bank account outside the country.
- Client accepts very unfavorable conditions unrelated to his or her health or age.
- Transaction involves use and payment of a performance bond resulting in a cross-border payment.
- The same beneficiary for multiple policies.
- Relationship between the policy holder and the beneficiary is not clearly established.

ML/TF indicators specific to businesses who provide loans

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 if you are involved in the business of providing loans (including mortgages) or extending credit to individuals or corporations. Below are some examples of sector specific ML/TF indicators that you should consider as part of your STR program.

- Client suddenly repays a problem loan unexpectedly.
- Client makes a large, unexpected loan payment with unknown source of funds, or a source of funds that does not match what you know about the client.
- Client repays a long-term loan, such as a mortgage, within a relatively short time period.
- Source of down payment is inconsistent with borrower's background and income.
- Down payment appears to be from an unrelated third party.
- Down payment uses a series of money orders or bank drafts from different financial institutions.
- Client shows income from "foreign sources" on loan application without providing further details.
- Client's employment documentation lacks important details that would make it difficult for you to contact or locate the employer.
- Client's documentation to ascertain identification, support income or verify employment is provided by an intermediary who has no apparent reason to be involved.
- Client has loans with offshore institutions or companies that are outside the ordinary course of business of the client.
- Client offers you large dollar deposits or some other form of incentive in return for favorable treatment of loan request.
- Client asks to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known.
- The loan transaction does not make economic sense (for example, the client has significant assets, and there does not appear to be a sound business reason for the transaction).
- Client seems unconcerned with terms of credit or costs associated with completion of a loan transaction.
- Client applies for loans on the strength of a financial statement reflecting major investments in or income from businesses incorporated in countries known for highly secretive banking and corporate law and the application is outside the ordinary course of business for the client.
- Down payment or other loan payments are made by a party who is not a relative of the client.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

1.4.1 Enrolment with FINTRAC's electronic reporting system

The compliance officer is required to ensure we are enrolled with FINTRAC's electronic reporting system, F2R system, to report electronically. Once enrolled, FINTRAC provides an identifier number to include in our reports. This number is retained by the compliance officer.

The compliance officer submits all reports to FINTRAC.

Contact information for enrollment:
(http://www.fintrac-canafe.gc.ca/reporting-declaration/Info/f2r-eng.asp)

Toll-free: 1-866-346-8722 and pressing <4> after choosing your language

Financial Transactions and Reports Analysis Centre of Canada
234 Laurier Avenue West, 24th floor
Ottawa ON K1P 1H7
Canada

Confidentiality and immunity

You are not allowed to inform anyone, including the client, about the contents of a suspicious transaction report or even that you have made such a report. This applies whether or not such an investigation has begun.

Since it's important not to tip your client off that you are making a suspicious transaction report, we should not be requesting information from the individual conducting or attempting the transaction that we would not normally request during a transaction.

No criminal or civil proceedings may be brought against anyone for making a report in good faith concerning a suspicious transaction.

1.4.2 – Large cash transaction reporting and record keeping policy

Requirement – A report must be submitted and a record created and retained for every amount of cash of $10,000 or more received from a client in a single transaction for non-registered annuities, non-registered investments or universal life insurance policies Other products are exempt from large cash transaction reporting. If we know that two or more cash transactions of less than $10,000 each were made within a 24-hour period (that is, 24 consecutive hours), by or on behalf of the same client, these are considered to be a single large cash transaction if they add up to $10,000 or more.

Policy – We do not accept cash from clients and as such we will not be required to submit a large cash transaction report or keep a record.

Procedures –
Clients offering to provide cash for the payment of transaction are provided alternative payment options. All financial instruments used for payment of insurance policies are payable to the insurance company and are provided to the insurer.

If cash was accepted in error the following actions will be followed:

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

The compliance officer is required to:

- Submit large cash transaction reports within 15 calendar days of the transaction taking place
- Create and retain a large cash transaction record
- Retain copy of the large cash transaction records in a secure location

Information to include on a large cash transaction report
See FINTRAC's Guideline 7A *Submitting large cash transactions reports to FINTRAC* for details of what information needs to be included in a large cash transaction report.

Information to retain on a large cash transaction record
See FINTRAC's Record keeping requirements for Large cash transaction records for the information required to be kept in a large cash transaction record.

1.4.3 – Terrorist property reports

Requirement – If we have property in our possession or control that we know or believe is owned or controlled by or on behalf of a terrorist group we must report to FINTRAC without delay.

Policy –We do not accept cash or hold funds on behalf of clients, and funds from clients are made payable to the insurer. We also do not hold property on behalf of clients. Accordingly, we should not have property in our possession or control.

All instances of terrorist property in our possession or control are brought forward to the compliance officer. Information and FINTRAC requirements are outlined below for reference, should such instances arise.

Procedures – The compliance officer submits the report to FINTRAC and notifies the RCMP. Terrorist reports must be submitted by paper to FINTRAC. Forms are available as follows:

- **Reporting forms** can be accessed and printed from FINTRAC website.
- Call 1-866-346-8722 for a copy to be faxed or mailed to you.

When a report is required to be filed we review FINTRAC Guideline 5 *Submitting terrorist property reports* for details of what each field must contain for a terrorist property report.

Section 2 – Client information record keeping

2.1 – General

During the establishment of an applicable insurance policy, applications and forms are used to collect required client information.

Individual client information collected may include as required, but is not limited to, their identification, occupation, industry, employment, address, tax residency, date of birth, source of wealth, intended use of the policy, third party involvement and any known political exposure.
For clients which are legal entities, additional information is required which provides the information on the beneficial owners of the entity and those who control the entity, as specified in FINTRAC guidance and outlined below.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

2.2 – Client information record

Policy – Client information records are maintained for all clients (individuals and entities) that are expected to pay more than $10,000 (whether or not it's in cash) for non-registered annuities, non-registered investments or universal life insurance policies. Other products are exempt from client information record requirements.

Procedures – In practice we comply with the obligation to create a client information record by completing insurer applications for insurance products, which capture all of the required information. Information retained in client information records vary depending on the type of client (individual or entity) and the nature and/or volume of the client's transactions. Key components of client information records include:

- Client identification information (individuals and entities)
- Industry and occupation (business type for entities)
- Beneficial ownership information (entities)
- Third party determination and information
- Politically exposed person determination (for $100,000 lump sum deposit is provided)
- Business relationship information (purpose and intended use of the policy)

Details of what is required for each component of the client information record are outlined in Section 2.3.

2.3 – Summary Chart

Client information record component	When required	Information required to be recorded/retained
Client information for individuals – Recorded on applications & forms.	In all occasions where the life insurance policy has cash values, and non- registered investment accounts	**Client information:** • Name • Address • Date of birth • Industry and occupation (descriptive) **Client identification details:** • Identification details (including details of type, identifying number, place of issue, expiry) **see Section 3 Client identity for details of required information*
Client information and beneficial ownership and control records for entities – Recorded on applications, forms and copies retained of supporting documentation from the client. ** See below for definitions and additional policy and procedure information.*	If the owner is an entity and or other than the applicant him or herself	**Client information for all types of entities:** • Entity name • Address • Incorporation or other identifying number • Jurisdiction of incorporation • Detailed description of the entity's principal business and industry • Signatory information (name, address, DOB, occupation, identification [including details of type, identifying number, place of issue, expiry]) **Information to confirm existence of an entity**

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

		and beneficial ownership, structure and control information;
		• Copies of documents used to confirm existence such as:
		  ○ Certificate of corporate status (corporations)
		  ○ Notice of assessment issued by municipal, provincial, territorial or federal government (corporations)
		  ○ Partnership agreement (entity other than a corporation)
		  ○ Articles of association (entity other than a corporation)
		• Copies of records obtained to confirm information about the individuals who ultimately control the entity, ownership and provisions relating to power to bind such as:
		  ○ Articles of incorporation/association
		  ○ Shareholder or partnership agreements
		  ○ Annual return (T1 Sch50 or equivalent)
		  ○ Bylaws of the corporation
		  ○ Certificate of incumbency
		  ○ Trust deed
		  ○ Evidence of power to bind
		• Names of all directors (for corporations)
		• Names and addresses of trustees, known beneficiaries and settlors of the trust (for trusts)
		• Names and addresses of all individuals/entities who directly or indirectly own or control 25% or more of the entity (for entities other than trusts)
		• Information establishing the ownership, control and structure of the entity.
		
		If this information cannot be obtained or accuracy not confirmed record:
		• Name of the most senior managing officer of the entity and ascertain their identity and treat the client as high risk
		
		Not-for-profit organization requirements
		Determine whether or not the entity is a registered charity for income tax purposes. If it's not a registered charity, determine whether or not it solicits charitable financial donations from the public.

Third Party information determination – Recorded on applications and forms. ** See below for definitions and*	If the payor is an entity or other than the owner If the named beneficiary has no reasonable financial interest with the insured	• Third party determination – is there a third party involved with interest or control of the policy? Yes or no is recorded on applications and forms. If yes, the following is collected; • Name and address of third party

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

additional policy and procedure information.		• Occupation or principal business of third party • Date of birth (if an individual) • Incorporation number and place of incorporation (if a corporation) • Nature of relationship between third party and client If involvement of a third party is suspected even though the client has declared there is not a third party involved, document why we suspect the individual is acting on a third party's instructions
Politically exposed person (PEP) or Head of an International organization (HIO) determination – Recorded on applications and forms. ** See below for definitions and additional policy and procedure information.*	Mandatory For the contributor of deposits $100,000 or greater for life insurance, and For all life insurance policy that has cash value	• PEP determination – is client a PEP or HIO (includes close relatives/close associates)? Yes or no recorded-on applications and forms. If yes; • The name, relationship and office/position of the individual who is a PEP and country • The source of the funds, if known, that were used for the transaction • The date you determined the individual to be a PEP or HIO • The name of the member of senior management who reviewed the transaction • The date the transaction was reviewed
Business relationship information – Recorded on applications and forms. ** See below for definitions and additional policy and procedure information.*	When we conduct two or more transactions in which we have to ascertain ID or confirm existence of an entity we have entered into a business relationship with the client.	Record of the purpose and intended nature of the business relationship on applications and forms (e.g., financial planning, estate planning, capital preservation etc.).

2.3.1 Beneficial ownership and control records

What is beneficial ownership and control? Beneficial ownership refers to the identity of the individuals who **ultimately control, either directly or indirectly 25% or more of** the corporation or entity (shares or rights). The indirect ownership reference is important as it requires that a legal entity owned by another corporation or another entity may require additional documentation to confirm that all beneficial owners have been disclosed.

Policy – When confirming the existence of an entity, reasonable measures must be taken to confirm and keep records of the information about the entity's beneficial ownership. Information is documented on applications and forms. Copies of all documentation used to obtain/confirm beneficial ownership and control (such as those listed in the table above) are retained in the client file.

Procedures – We must search through as many levels of information as necessary in order to determine beneficial ownership. However, there may be cases where there is no individual who owns or controls 25 per cent or more of an entity. We must still keep a record of the information obtained.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

Reasonable measures to confirm the accuracy of beneficial ownership information would include asking the client to provide suitable documentation, or refer to publicly available records as detailed in the chart in Section 2.2 of this program. Documents that we obtain to confirm the information or the public source i.e., the website where we found the information have to be kept in our records.

We do not need to ascertain the identity of the most senior managing officer when there is no individual who owns or controls 25 per cent or more of an entity.

If the client refuses to provide the beneficial ownership of the legal entity when a beneficial owner exists, then the client must be considered high risk and additional identification of the most senior managing officer is required. A decision may also be made not to proceed with doing business with this client without this information.

Examples of ownership, control and structure can be found in Fintrac's Guidance, Know your client - Beneficial ownership requirements - Appendix A

2.3.2 Third party determination and records

Who is a third party? – A third party is an individual or entity other than the individual or entity who conducts the transaction such as a payor, power of attorney or someone directing the transaction. When determining whether a third party is involved, it is not only about who "owns" the money, but rather about who gives instructions to deal with the money. To determine who the third party is, the point to remember is whether the individual in front of you is acting on someone else's instructions. If so, that someone else is the third party.

Policy – We make a third-party determination (request the client to disclose if a third party exists) when we are required to keep a client information record. We are also required to make a third-party determination when we have to keep a large cash transaction record.

Procedures – How is a third-party determination made? At the time of application the client is asked whether **any other person or entity will be paying for this policy, will have the use of or have access to the policy values while it's in effect, or whether any other person is providing direction to apply for this policy?** The client's answer is documented on applications and forms. If there is a third party involved, required information about the third party is also recorded on applications and forms such as:

- Name and address of third party
- Occupation or principal business of third party
- Date of birth (if an individual)
- Incorporation number and place of incorporation (if a corporation)
- Nature of relationship between third party and client

When we have reasonable grounds to suspect that there is a third party involved we keep a record, on application and forms, to indicate the following:

- In the case of a client information record or a large cash transaction, whether, according to the client, the transaction is being conducted on behalf of a third party
- Why we suspect the individual is acting on a third party's instructions
- In the case of a large cash transaction, whether, according to the individual giving the cash, the transaction is being conducted on behalf of a third party

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

2.3.3 Politically exposed persons (PEP) or Head of international organization (HIO) determination and records

Who is a PEP? A PEP is an individual who holds or has ever held one of the following offices or positions subject to certain terms and expiry noted below:

- A head of state or government
- A member of the executive council of government or member of a legislature
- A deputy minister (or equivalent)
- An ambassador or an ambassador's attaché or counsellor
- A military general (or higher rank)
- A president of a state-owned company or bank
- A head of a government agency
- A judge of a supreme court or appellant court
- A leader or president of a political party in a legislature
- For domestic PEP's this also includes, a mayor or equivalent municipal leader
- The head of an international organization (HIO) (e.g. an organization formed by treaty by one or more states, See FINTRAC guidelines for examples)

A PEP also includes the close associates (persons with a personal or business relationship) and the following family members of the individual described above:

- Mother or father
- Child
- Spouse or common-law partner
- Spouse's or common-law partner's mother or father
- Brother, sister, half-brother or half-sister (that is, any other child of the individual's mother or father)

Terms and expiry

Foreign persons – if the person holds or has ever held (includes deceased) **Domestic persons –** if the person holds or has held the position in the past five years

Heads of international Organizations – Is a Person who is currently holding or held with in last 5years

Policy – If we receive a lump-sum payment of $100,000 from an individual for an annuity or a life insurance policy, we take reasonable measures to determine whether we are dealing with a PEP/HIO within 30 days after the transaction occurred. If the client is a PEP, within the 30 days we also have the transaction approved by the senior management within the practice.

Upon determination that the contributor is a PEP or HIO, a risk assessment is required to be performed. If the client is a foreign PEP, then they are immediately considered high risk. If any PEP or HIO is considered high risk, then the applicable special measures are required to be completed within 30 days of the transaction.

These special measures to be completed within 30 days include;

1. Reasonable measures to collect the source of funds of the transaction
2. Have the transaction approved by the senior management within the practice
3. Record all of the steps taken for the determination, review and approval

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

Example – If it takes five days after the transaction to make the determination that we are in fact dealing with a politically exposed foreign person, we have twenty-five days left to perform a client risk assessment, collect the source of funds and to get senior management to review the transaction.

Procedures – How is a PEP/HIO determination made? We ask the client if they are a PEP; yes or no answer is documented on insurer applications and forms. We may also consult a credible source of commercially or publicly available information about PEPs.
If the client is PEP we:

- Document the office/position of the individual who is a PEP
- Ask the client for and document the source of the funds that were used for the transaction
- Document the date we determined the individual to be a PEP
- Document the name of who reviewed/approved the transaction
- Document the date the transaction was reviewed

How often do we make a PEP/HIO determination?
Once determined that an individual is a PEP/HIO we will not have to do it again. However, if we initially determined that an individual was not a PEP/HIO, we must still take reasonable measures to determine whether we are dealing with a PEP/HIO for every $100,000 lump sum deposit to an insurance policy, since the client's status may have changed.

2.3.4 **Business relationship record**

What is a business relationship? A business relationship begins when we conduct two or more transactions in which we have to ascertain the identity of the individual or confirm the existence of a corporation or other entity within a maximum of five years from one another.

Policy – We keep a record of the purpose and intended use of the insurance policy.

Procedures – We record the purpose and intended nature of the business relationship on applications and forms.

Business relationships also trigger other obligations; see Ongoing monitoring and keeping client information up-to-date in Section 4.3 of this program for additional detail.

2.4 **– Reasonable measures**

Keep a record of any "reasonable measures" you have taken

What are reasonable measures?
The term "reasonable measures" refers to activities we undertake in order to meet certain obligations. For example, we must take reasonable measures to confirm beneficial ownership information, to determine whether we are dealing with a PEP or HIO, to determine whether the client is acting on the instructions of a third party, etc., as outlined in the policies and procedures. If – even after taking reasonable measures – certain information cannot be determined, gathered or confirmed, we have met the obligation.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

Reasonable measures must not be confused with, and do not apply to data elements that are mandatory, that is, where information must be obtained before the transaction or activity can be completed.

Documenting reasonable measures

A record is kept when reasonable measures were taken, but were unsuccessful. A reasonable measure is unsuccessful when you do not obtain a response, such as a yes or no and you're unable to make a conclusive determination. When reasonable measures are unsuccessful, we must record the following information:

- The measure(s) taken
- The date on which the measure(s) was taken
- The reason **why** the measure(s) was unsuccessful

We consider a client's refusal to provide, or our inability to obtain certain information as part of the overall assessment of client risk. **Retention**: Keep records of your unsuccessful reasonable measures for at least five years following the date they were created.

Section 3 – Ascertaining Client Identity

Policy – The identity of individuals is ascertained and/or the existence of entities is confirmed for non-registered annuities, non-registered investments or universal life insurance policies upon policy establishment. Other products are exempt from client identification requirements except where a suspicious transaction report has been filed, whereby the exemption is no longer applicable.

Client identification details are recorded on applications and forms.

See *section 3.1 of this program* for measures taken/procedures to ascertain the ID of individuals and *section 3.3 of this program* for measures taken/procedures to confirm the existence of entities.

3.1 Individuals

Procedure: To ascertain the identity of an individual, we refer to one of the following methods. The identity can be ascertained by the advisor or licensed assistant who is contracted with the agency or the insurer

1. Photo identification issued by government-Must be Authentic Valid and Current.

2. Credit File Method-Where the information must be valid and Current.

3. Dual Process Method-Where the information must be Valid and Current and from different reliable sources.

A valid foreign passport may also be acceptable, however additional records to confirm that the client meets the Canadian residency requirements may be required by the insurer.
If we are unable to obtain identification through documents listed above we consult FINTRAC's Guidance - Know your client - Methods to identify individuals and confirm the existence of entities for additional options.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

3.2 Confirming the existence of entities

Procedures – Entities include corporations, trusts, partnerships, funds and unincorporated associations or organizations.

To confirm the existence of a corporation refer to the following documents:

- The corporation's certificate of corporate status
- A record that has to be filed annually under provincial securities legislation
- Any other record that confirms corporation's existence. Examples include corporation's published annual report signed by independent audit firm, or notice of assessment for the corporation from municipal, provincial, territorial or federal government.

To confirm the existence of an entity other than a corporation, refer to a partnership agreement, articles of association or any other similar record that confirms the entity's existence.

The record we use to confirm an entity's existence can be paper or an electronic version. If the record is in paper format, we have to keep a copy of it. If the record is an electronic version, we have to keep a record of the corporation's registration number, the type and source of the record. An electronic version of a record has to be from a public source. Confirming verbally (such as by telephone), it is not acceptable as we have to refer to a record.

For example, we can get information about a corporation's name and address and the names of its directors can be obtained from a provincial or federal database such as the Corporations Canada database which is accessible from Industry Canada's website (http://www.ic.gc.ca). A corporation searching and registration service is also acceptable.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

3.3 Exceptions to client identification

Policy – Once the identity of an individual has been verified as noted above we do not have to ascertain their identity again if we recognize the individual (visually or by voice using caller authentication). If there are any doubts we ascertain identity again.

Section 4 – Risk based approach

4.1 – Risk assessment

What is a risk assessment – A risk assessment is an analysis of potential threats and vulnerabilities to money laundering and terrorist financing to which your business is exposed. The complexity of the assessment depends on the size and risk factors of your business; details are outlined in the following sections and more information can be referred to in FINTRAC's Risk based approach workbook for life insurance companies, brokers and agents.

Types of risk assessments

Within this practice a **business-based risk assessment** and a **relationship-based risk assessment** are completed.

Assessments are reviewed every two years as part of the program evaluation or sooner if there are changes in the practice such as our location, client base, products or services etc.

How we identify risks
The following categories are considered in the risk assessments:

- Products, services and how we deliver our products and services
- Geography of our business and clients
- Our clients
- Other relevant factors

Products and services
Some products and services are associated with higher levels of inherent ML/TF risk. Key product attributes that contribute to higher inherent risk levels are features that enable the accumulation of cash or investments (which may be used in the placement or layering stage of money laundering, and terrorist financing), the ease of withdrawals or transfers (which facilitate layering and integration) and the ability of third parties to transact using the product (which may facilitate any of the stages of money laundering and terrorist financing). Product attributes that are of lower risk would have penalties for early withdrawals, limited ability to withdraw and no opportunity to build up of cash values.

Delivery channel risks
A delivery channel is the medium that can be used to obtain a product or service, or through which transactions can be conducted. Delivery channels that allow non-face- to –face transaction have a higher risk; it's more difficult to ascertain the identity of clients. This method can be used to obscure the true identity of a client or beneficial owner.

Geographical risk
Geographical location impacts overall business risk. Geographical attributes that may contribute to a higher inherent risk level include:

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- Proximity to an area known for high crime rates is considered
- Client connections to high-risk countries
- Size/nature of area where client base reside i.e., small rural area where clients are known vs. large urban area where clients are unknown

Other factors

Other factors such as the operational structure of our business model are also considered i.e., number of employees, employee turnover, number of branches etc. Impact of new technology in the industry and our business is also considered.

Ministerial directives and transaction restrictions received from subscribing to Fintrac's mailing list or through insurer communications are reviewed and assessed to determine impact on our risk assessment.

Additional resources can be found on FINTRAC's website in Guidance - Compliance program - Guidance on the risk-based approach to combatting money laundering and terrorist financing.

How individual clients are risk assessed (initially and ongoing)

Clients are risk assessed/assigned a risk rating when a new client relationship begins and are reassessed on an ongoing basis during monitoring.

Clients within this practice can generally be grouped into two groups:
Group A – Low risk
Group B – High risk

All clients default to low risk, **UNLESS risk factors are present such as;**
Automatic high-risk characteristics – if any of the flags below are present the client is high risk.

- Politically exposed foreign persons
- A client where a suspicious transaction, terrorist financing report has been filed
- A client who is an identified terrorist
- A client for whom we are unable to obtain beneficial ownership information
- A client with transactions sent to or received from North Korea (regardless of amount)

Potential high-risk triggers –Any one trigger may be enough to assess a client as high risk, and typically if three or more triggers are present the client should default to high risk. This can vary depending on our knowledge of other factors about the client's profile such as the products they hold, tenure with client, source of funds etc.

Client characteristics, product, service, delivery channel:

- Politically exposed domestic person, head of international organization and close associates
- Premium payments/deposits via wire orders from foreign jurisdictions
- Third party involvement without reasonable justification
- Occupation – High-risk occupations (i.e., cash intensive businesses, off shore business, business in high risk countries, online gambling)
- Client's business structure or transactions seems unusually complex
- Non face-to-face client identification without justifiable reason

Geography:

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

- Client resides outside local or normal customer area
- Client resides in known crime area
- Client has off-shore business activities, client connections to high-risk countries

Other suspicious transaction indicators:

- Volume/timing/complexity of transactions inconsistent with purpose of the policy/account
- Value of deposits inconsistent with occupation or source of funds
- Presence of any suspicious transaction indicators outlined in Part A "Background information" section

All high risk client assessments are documented using the *Client risk assessment tool* located in the appendix of this program. Copies are retained to demonstrate the client has been assigned the appropriate risk.

4.2 **– Risk mitigation**

Where high risks have been identified in our risk assessments, risk mitigation measures have been developed and are in place. Risk mitigation measures are detailed in the risk assessments in Section 4.4 and 4.5 of this program.

4.3 **– Ongoing monitoring and keeping client information up-to-date**

Once a business relationship is established we must:

- Conduct ongoing monitoring of our business relationships
- Keep client information up-to-date

The purpose of ongoing monitoring and keeping client information up-to-date is to:

- Detect suspicious transactions that have to be reported
- Reassess the level of risk associated with the client's transactions and activities
- Determine whether the transactions or activities are consistent with the information previously obtained about the client, including the risk assessment of the client
- Continue to understand the clients activities

For an individual during ongoing monitoring confirm/update the following information:

- The individual's name
- Address
- Occupation or principal business

For entities confirm/update the following information:

- Name
- Address
- Principal business or occupation
- Name of directors, trustees etc.
- Beneficial ownership information (Information on the individuals who ultimately control the entity)

Frequency – The frequency with which we conduct ongoing monitoring of business relationships and update client information depends on the clients risk rating with high-risk clients being monitored/updated more frequently.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

Low-risk clients – Transactions are monitored/reviewed/assessed when they are conducted. Client information can be kept up-to-date by verbally confirming information with clients periodically during ongoing interactions (i.e., new business or subsequent transactions).

High-risk clients – Transactions are monitored/reviewed/assessed when they're conducted as well as during periodic reviews. Evidence of the periodic review is maintained. Notes are also maintained in the client file.

Client identification information is updated annually. Information can be verbally confirmed with the client. Additional measures **may** include taking reasonable measures to confirm information provided by high-risk clients by conducting internet searches.

4.4 **– Business based risk assessment**

Listed below are the areas where this practice may be vulnerable to being used by criminals for conducting money laundering or terrorist financing (ML/TF) activities. This list takes into consideration the products and services we provide, how we deliver the products or services and the location of our practice. This list is updated with additional risks as identified. All factors assessed as high must have risk mitigation measures.

LIST OF FACTORS **Frequency/ business impact** ***Identify all the factors that apply to your business (i.e., products, services and delivery channels, geography, other relevant factors) and indicate the frequency or whether the risk is present in your practice.***	**INHERENT RISK RATING** ***Assess each factor as high or low.***	**RATIONALE** ***Explain WHY risk rating was assigned.***	**For all HIGH risks identified in the first column describe MITIGATION MEASURES that will be carried out to reduce the risk of money laundering and/or terrorist financing.**
Products and Services			
Non-registered investments and annuities Frequency sold in this practice ____Frequently ____Occasionally ____Rarely/Never	HIGH	Ability to accumulate investments, ease of withdrawals and transfers, ability for third parties to transact using the product.	Cash is not accepted; would not be exposed to the placement stage of money laundering. Obtain source of funds for all clients. Training for employees to ensure an understanding of the products that are sold and the risk of ML/TF that is present with these products and related transactions.
Universal life	HIGH	Ability to accumulate	Cash is not accepted; would

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

Frequency sold in this practice ____Frequently ____Occasionally ____Rarely/Never		investments, ease of withdrawals and transfers, ability for third parties to transact using the product, transfer of ownership, ability to over pay	not be exposed to the placement stage of money laundering. Obtain source of funds for all clients. Training for employees to ensure an understanding of the products that we sell and the risk of ML/TF that is present with these products and related transactions.
Whole life Frequency sold in this practice ____Frequently ____Occasionally ____Rarely/Never	LOW	Exempt product subject to tax exempt rules and monitoring	Not required as risk assessed as LOW
Term Frequency sold in this practice ____Frequently ____Occasionally ____Rarely/Never	LOW	Exempt product. No buildup of cash value, no ability to withdraw or repayment of contributions.	Not required as risk assessed as LOW
Group insurance Frequency sold in this practice ____Frequently ____Occasionally ____Rarely/Never	LOW	No cash surrender value or saving component.	Not required as risk assessed as LOW
Registered investments/annuities ____Frequently ____Occasionally ____Rarely/Never	LOW	Exempt product.	Not required as risk assessed as LOW
Delivery channels			
Face to face (on-boarding and ongoing transactions) Frequency this delivery channel is used by clients	LOW		Not required as risk assessed as LOW

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

____Frequently ____Occasionally ____Rarely/Never			
Non face-to-face delivery channels (telephone, email, Skype, etc.) Frequency this delivery channel is used by clients ____Frequently ____Occasionally ____Rarely/Neve	HIGH	Identifying clients that are not physically present is higher risk as it is more difficult to be certain who the client is and who you are transacting with.	Arrange opportunity to meet with client in person in the future before entering into two transactions requiring ID (business relationship). Not accept new client if they are unwilling to meet face to face without justifiable reason such as distance, inability to travel i.e. disability.
Geography			
Business conducted in areas that are not within close proximity to a border town. ____Frequently ____Occasionally ____Rarely/Never	LOW	Financial institutions that are not located within close proximity to a border crossing are less likely to be the first point of entry for funds into the financial industry.	Not required as risk assessed as LOW
Business conducted in areas within close proximity to a border town. ____Frequently ____Occasionally ____Rarely/Never	HIGH	Financial institutions located within close proximity to a border crossing may be more likely to be the first point of entry for funds into the financial industry. Clients who live in close proximity to a border town may also have more connections to the import/export sector and potentially have sources of funds in other countries.	Cash is not accepted and as such we would not be the first point of entry. Obtain source of funds for all clients.
Business conducted in geographic location(s) known to have low presence of crime? ____Frequently ____Occasionally ____Rarely/Never	LOW	Low presence of crime reduces the risk that source of funds may be from illegal activities.	Not required as risk assessed as LOW

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

Business conducted in geographic location(s) known to have high presence of crime? ____Frequently ____Occasionally ____Rarely/Never	HIGH	Areas with higher crime may have clients with sources of funds from criminal activities.	Obtain source of funds for all clients. On a regular basis information available online regarding crime in our area is reviewed. Sources such as Statistics Canada provide information on crime in Canada by type and region. As necessary training is provided to employees to ensure they are aware of the types of crime in our area and remind them of due diligence at on-boarding such as occupation and source of funds.
Business conducted in smaller city where clients are often known at time of on-boarding? ____Frequently ____Occasionally ____Rarely/Never	LOW	This practice operates in a smaller city and/or clients are often known at time of on-boarding?	Not required as risk assessed as LOW
Business conducted in a large city where new clients are typically unknown to the practice at the time of on-boarding? ____Frequently ____Occasionally ____Rarely/Never	HIGH	In a larger city there is potentially more new client anonymity where clients are often unknown to the practice at time of on-boarding.	Obtain source of funds for all clients. Ensure that we meet in person with all clients before entering into a business relationship.
Are there connections to high-risk countries, i.e., wire transfers received from foreign countries that potentially pose a risk of ML/TF? Frequency of occurrence in this practice ____Frequently ____Occasionally ____Rarely/Never	HIGH	Transactions such as wire transfers from foreign jurisdictions are potentially a higher risk for ML/TF.	Obtain source of funds for all clients. Reassess the level of risk associated with the client as transactions occur. Review the sanctioned countries listing annually or as notified of updates to the listing through FINTRAC and/or insurer communications to ensure awareness of high-risk countries. These are

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

			available on the Office of the Superintendent of Financial Institutions' website (http://www.osfi-bsif.gc.ca), by referring to the "Terrorist Listings and Sanctions" link.
Other risk factors			
Business model - established practice, trained employees, low employee turnover and consistent geographic location ____Reflects my current practice ____Does not reflect my current practice	LOW	Characteristics such as low number of employees and/or low employee turnover, one office location with little anticipated change in geography, products or client base.	Not required as risk assessed as LOW
Business model - Larger practices with several employees and/or high turnover that impacts training requirements and practices that may be experiencing changes to their location of client bases may be at an increased risk. ____Reflects my current practice ____Does not reflect my current practice	HIGH	This practice has some higher risk factors such as: several employees, different roles, different training needs, several office locations or anticipated changes to geography, products and/or client base.	Ensure training of all new employees occurs before they have interactions with clients. When changes in risk i.e. geography, products or clientele we update training materials to ensure all members in the practice are aware of new risks presented.

4.5 **– Relationship based risk assessment**

Business *relationships* *Identify all your business relationships or high-risk clients (individually or as groupings) and assess as low or high*	**Rationale** *Explain why you assigned that particular rating*	**Describe enhanced measures** to ascertain ID for high-risk business relationships	**Describe mitigation measures, enhanced ongoing monitoring and process to keep client information up-to-date** for high-risk business relationships
Group A – LOW	Clients that conduct transactions face-to-face, or non-face-to-face with justifiable reason, in line with the client's profile i.e., occupation, source of	N/A	N/A

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

	funds, purpose of the policy etc., that do not have any automatic high-risk triggers.		
Group B – HIGH	Clients for whom suspicious transaction reports have been previously submitted as reasonable grounds for suspicion have already been established. Politically Exposed Foreign Persons (PEFP) as a PEFP may be vulnerable to ML/TF or corruption due to their position, relationship or influence. Clients for whom we are unable to obtain beneficial ownership information. This may indicate that the client is trying to hide the beneficial owner. A client that is an identified terrorist. A client with transactions sent to or received from North Korea (regardless of amount) Clients with a combination of potential high-risk triggers at on-boarding or as noted during ongoing monitoring that have been assessed and determined to be high risk. Potential high-risk triggers are listed in the risk assessment tool – See appendix.	**Enhanced ID measures** Ensure ID is ascertained at time of application with a valid piece of photo identification issued by a federal or provincial government.	**Mitigation measures may include:** • Completion of the *Client risk assessment tool (see appendix)* documenting rationale for assessment. • Perform an internet search of the client to see if there is any adverse media. **Keeping information up-to-date:** • Confirm/update client identification information with the client at every transaction and perform subsequent online searches. **Enhanced ongoing monitoring** • Review each transaction made by high risk clients at the time the transaction is conducted. - Maintain notes detailing the review of client transactions. - Compare the transaction to the purpose and nature of the business relationship. - Evaluate transaction against the client's profile. - Request additional information from client if transaction seems inconsistent with client profile. • Periodic review of client transactions

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

Section 5 – Timeframe for keeping records

We keep the following records for 5 years from the day the last business transaction was conducted:

- Client information records (including individual client identification)
- Records to confirm the existence of an entity
- Beneficial ownership records
- Politically exposed foreign person determination records
- Third party determination records

We keep copies of suspicious transaction, large cash and terrorist property reports we have filed for at least five years following the date the report was made.
All other records are kept for at least five years following the date they were created.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

PART D –TRAINING PROGRAM

All individuals within this practice who:

- Have contact with clients
- Who see client transaction activity
- Who handle cash or funds
- Who are responsible for implementing and overseeing the compliance regime, are trained as outlined in this training program to ensure an understanding of their obligations

Frequency – Training is mandatory for all new employees before they interact with clients. Training is an ongoing process. AML/ATF update training takes place annually or more frequently if needed based on changes to legislation, new products, changes in services offered, geography or delivery channels.

Method – Training is completed through circulation and review of Section A – background information and Section C – Policies and procedures of this compliance program. Optional/additional training may include modules provided by insurers, circulation of AML communications/updates from insurers, news article, FINTRAC communications etc. Types of training delivered are recorded on the tracking sheet below.

The compliance officer facilitates and tracks completion of all training on the attached chart. Records of completed training are retained in this section of the compliance program.

Training completion tracking

Employee name	**Type of training and content (initial training, ongoing review of policies procedures and background information, module provided by insurer, etc.)**	**Date**	**Employee signature**
Example – Cam Smith	*Initial training, review of policies procedures and background information*	*Dec. 1, 2020*	

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

PART E – APPROVAL AND ADOPTION OF POLICIES, PROCEDURES AND TRAINING PROGRAM

The policies, procedures and training program documented in this compliance program have been approved and adopted by the principal/owner of this practice.

Name of principal/owner: _____

Date this program was adopted: _____

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

PART F – PROGRAM REVIEW

Policies

A review of policies and procedures must be completed every two years. The compliance officer completes the program review.

Should the practice experience a major change, a program review may be completed before the two-year period has expired. Changes that may trigger an early audit are the purchase of a book of business, legislative/regulatory changes, opening a new office/branch, or noticeable demographic shifts in clientele.

The principal signs the results of the program review within 30 days of completing the review.

Program Review		
Completed by:		**Date**
Results reviewed by:		**Date**
Compliance item reviewed	**Yes/No**	**Results of testing**
1) Appointment of a compliance officer		
Testing includes: a) Ensure a compliance officer has been appointed and approved by senior management	Yes	A compliance officer has been appointed as indicated in the program and the appointment has been approved by the principal as indicated in the compliance officer section of this program.
2) Written compliance policies and procedures are approved, effective and reflect current legislative obligations		
Testing includes: a) Confirm policies and procedures have been approved by the principal.	Yes	Policies and procedures have been approved by the principal as indicated in Part E - Approval and adoption of policies, procedures and training program.
b) Refer to the FINTRAC website to see if there are new legislative changes noted. If there are changes since the date of last review/revisions to this program, make updates as required to ensure program is up to date with FINTRAC guidelines.	Yes	Reviewed website, legislative changes effective Jan 2019, Oct 2019, June 2020 & June 2021 are incorporated in this program.
c) If any reports have been made to FINTRAC ensure appropriate records have been retained.	NA	We have not had any circumstances arise requiring reporting to FINTRAC.
d) Review the business-based and relationship-based risk assessments to ensure that all risk categories have been considered i.e. geography, products, services, delivery channel & other factors & that assessments accurately reflect your business and	Yes	Risk assessments include all categories.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

client base.		
e) Review all high risks identified in both assessments to ensure risk mitigation measures have been developed and are appropriate to mitigate risk.	Yes	Risk mitigation measures have been documented and implemented.
f) Review 10% of high-risk clients to see if enhanced measures have been conducted i.e., periodic review.	Yes NA	Reviewed 10% of high risk clients, evidence of periodic review was noted. OR At this time there are no high risk clients identified in the practice
3)Program review has been completed at least every two years and results reviewed		
Testing includes: a) Confirm that a program review has been completed within the past two years	N/A YES	Implementation of this program replaces the existing program for this practice and as such as program review has not been completed in the past two years. Next program review will be scheduled for two years after implementation of this program or sooner if needed as noted in policies above. OR This program is the first program documented for the practice, a self-review will be completed within two years. OR A self-review was completed within the past two years, the next self-review will be scheduled for two years from implementation of this program.
b) Confirm the review was signed off by the principal.	Yes	The results of this review were signed off as indicated above.
4)Ongoing compliance training – policies and procedures for the frequency and method of training are in place and effective		
Testing includes: a) Ensure frequency of training is detailed in the program.	Yes	The training program states that training will occur annually.
b) Ensure all employees that have exposure to client transactions have received training annually by viewing evidence of training completion.	Yes	Evidence of training maintained and reviewed to ensure that all required employees have received training.
Actions required No actions required at this time.		
Follow-up actions completed		

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

PART G – REVISION HISTORY

Date	Section changed	Reason for change

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

APPENDIX

Client risk assessment tool

This tool is used to document client risk assessments when automatic high-risk characteristics are present and/or potential high-risk triggers are present when on-boarding and/or monitoring.

Document in the space below the rationale for client risk rating.

Automatic high-risk characteristics – if any of the flags below are present the client is high risk.

- Politically exposed foreign persons
- A client where a suspicious transaction, terrorist financing report has been filed
- A client who is an identified terrorist
- A client for whom we are unable to obtain beneficial ownership information
- A client with transactions sent to or received from North Korea (regardless of amount)

Potential high-risk triggers –Any one trigger may be enough to assess a client as high risk, and typically if three or more triggers are present the client should default to high risk. This can vary depending on our knowledge of other factors about the client's profile such as the products they hold, tenure with client, source of funds etc.

Client characteristics, product, service, delivery channel:

- Politically exposed domestic person, head of international organization and close associates
- Premium payments/deposits via wire orders from foreign jurisdictions
- Third party involvement without reasonable justification
- Occupation – High-risk occupations (i.e., cash intensive businesses, off shore business, business in high risk countries, online gambling)
- Client's business structure or transactions seems unusually complex
- Non-face-to-face client identification without justifiable reason

Geography:

- Client resides outside local or normal customer area
- Client resides in known crime area
- Client has off-shore business activities, client connections to high-risk countries

Other suspicious transaction indicators:

- Volume/timing/complexity of transactions inconsistent with purpose of the policy/account
- Value of deposits inconsistent with occupation or source of funds
- Presence of any suspicious transaction indictors outlined in Part A "Background information" section

Document your assessment and rationale here. Notes from ongoing monitoring can also be recorded here.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535

Updated AML/ATF Modules to include Amendments to Canada`s Anti-Money Laundering and Anti-Terrorist Financing Legislation effective June 1, 2021

Introduction

In 2018, we added the AML/ATF Modules to the Compliance section of the Advisor website to assist advisors with their AML/ATF compliance programs. The modules focus on each of the five compliance program requirements required by FINTRAC and provide guidance and templates to help advisors develop or enhance their compliance programs.

We are pleased to announce that we have amended our AML/ATF Modules to align with FINTRACs new regulatory amendments that took effect June 1, 2021.

A high level summary of some of the specific changes for insurance companies, brokers, and agents include:

Politically Exposed Persons (PEP) and Heads of International Organizations (HIO)

The changes to the obligations life insurance companies, brokers, and agents have regarding PEP/HIO screening, monitoring, and recordkeeping include:

- Taking reasonable measures to determine whether someone who makes a lump-sum payment of$100,000 or more in funds with respect to an immediate or deferred annuity or life insurance policy is a PEP, HIO, or a family member or a close associate of a PEP or HIO. If the person is determined to be a foreign PEP or a domestic PEP or HIO that is determined to be high risk you must take reasonable measures within 30 days to establish the source of the funds and the source of the person's wealth, and ensure that a member of senior management reviews the transaction.
- Taking reasonable measures to determine whether any person to whom is remitted $100,000 or more over the duration of an immediate or deferred annuity or life insurance policy is a PEP, HIO, or a family member or a close associate of a PEP or HIO.
- When reviewing transactions involving a PEP, HIO, or family member or close associate of a PEP or HIO, a record must be kept, including specific details about the PEP/HIO, the date of the determination, the source of the funds, the source of the person's wealth, the name of the entity's senior management who reviewed the transaction and the date of the review. Transaction records must be kept for at least five years from the day on which the business transaction was conducted.

Recordkeeping Requirements

Life insurance companies, brokers and agents will be subject to new recordkeeping requirements under the Amendments. Changes under the new guidance include:

- Must retain records of terrorist property reports, large cash transaction reports for five years
- Records of unsuccessful reasonable measures are no longer required
- Large virtual currency transaction records do not need to be kept if the amount was received from a financial entity or public body or a person acting on behalf of a financial entity or public body.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951 Fax: (888)511-3535

On-going Monitoring Requirements

The new guidance provides that the requirements for enhanced ongoing monitoring end when the business relationship ends or the client is no longer high-risk. This is significantly less burdensome than the ongoing monitoring obligations under prior guidance which required that Reporting Entities perform enhanced monitoring for high-risk clients for five years after the closure of the account.

Additionally, under the new guidance, insurance companies, brokers and agents do not have to conduct ongoing monitoring when dealing in reinsurance.

Methods to Identify Individual and Entities

The guidance regarding acceptable methods to verify the identity of individuals and entities has been updated. The updated guidance largely contains minor changes to the prior guidance. One specific change includes, if a child is between 12 and 15 years of age, you can verify their identity by using any of the methods prescribed by FINTRAC. If this is not possible due to a lack of identification information, you may use a variation of the dual-process method that allows you to:

- Refer to one reliable source of information that includes the name and address of the child's parent, guardian, or tutor; and
- Refer to a second reliable source that includes the child's name and date of birth.

For further information on advisor obligations for AML/ATF, please go to www.fintrac.gc.ca.

220-1550 South Gateway Road Mississauga ON L4W 5G6. Cell: (647) 920-4951
Fax: (888)511-3535