# COMPLIANCE PROGRAM FOR ANTI-MONEY LAUNDERING AND ANTI-TERRORISM FINANCING

**B&A and Associates Insuarnce Agency Limited.**

# 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. 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.

### 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 detecting and deterring terrorist financing.

## 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

### 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 Administrative Monetary Penalties Regulations* by degree of importance 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.

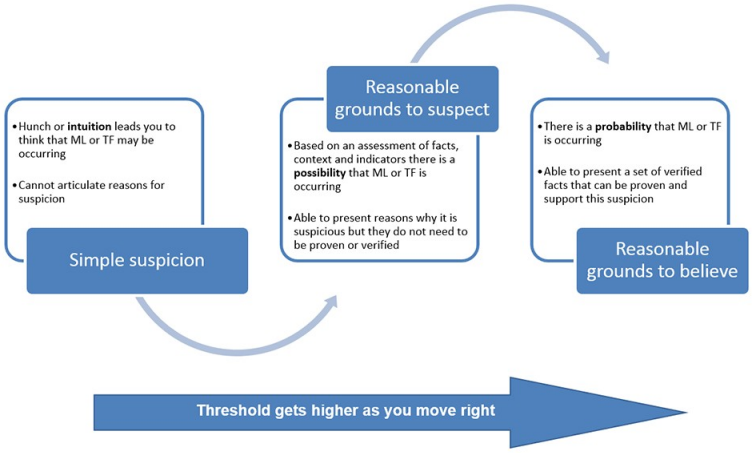
## v) Reasonable grounds to suspect

You must report a transaction as suspicious as soon as practicable after taking measures that have given you reasonable grounds to suspect that a transaction is related to the commission or attempted commission of an ML/TF (money laundering/terrorist financing) offence.

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

Reasonable grounds to suspect is more than simple suspicion. You can only arrive at the conclusion you have reasonable grounds to suspect after you've assessed facts, context and ML/TF indicators associated with the financial transaction. Your suspicion must be reasonable and not biased or prejudiced.

Understanding the differences between the thresholds can help to clarify what reasonable grounds to suspect means and reasonable grounds to suspect can be used within a compliance program. See the diagram below for a visual overview of the following thresholds.




**Simple suspicion** is a lower threshold than reasonable grounds to suspect and is synonymous with a "gut feeling" or "hunch". Simple suspicion means that you have a feeling that something is unusual or suspicious, but do not have any facts, context or ML/TF indicators to support that feeling or determine if there are reasonable grounds to suspect the occurrence of an ML/TF offence. Simple suspicion could prompt you to assess related financial transactions to see if there are additional facts, context or ML/TF indicators that would support/confirm your suspicion.

**Reasonable grounds to suspect** is the required threshold for submitting an STR to FINTRAC and is a step above simple suspicion, meaning that there is a **possibility** of an ML/TF offence.

Reaching reasonable grounds to suspect means that you considered and reviewed the facts, context and ML/TF indicators related to a financial transaction and concluded that

you have reasonable grounds to suspect that this particular financial transaction is related to ML/TF. You must be 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.

You **do not** have to verify the facts, context or ML/TF indicators that led to your suspicion, nor do you have to prove that an ML/TF offence has occurred in order to have reasonable grounds to suspect.

The explanation of your assessment should be included in the narrative portion, Part G, of the STR. In your report to FINTRAC, include all the factors that support your assessment and conclusion that an ML/TF offence has possibly occurred.

**Reasonable grounds to believe** is a higher threshold than reasonable grounds to suspect and is **beyond** what is required to submit an STR. Reasonable grounds to believe means that there are verified facts to support the **probability** that an ML/TF offence has occurred. In other words, there is enough evidence to support a reasonable and trained person to **believe**, **not just suspect**, that ML/TF has occurred. For example, law enforcement must reach reasonable grounds to believe that criminal activity has occurred before they can obtain judicial authorizations, such as a production order.

### vi) Indicators of suspicious transactions or potential high-risk clients

The following are some examples of 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. Criminal organizations often combine various methods in novel ways in order to avoid the detection of ML/TF. 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.

On its own, a single indicator may not appear suspicious. However, observing an indicator(s) could lead to an assessment of the transaction(s) to determine whether there are further facts, contextual elements or additional ML/TF indicators that might require the submission of an STR.

**General indicators**
The following are 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 is typically not just one of these factors alone that would form the reasonable grounds to suspect, 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 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
- Client may be the owner of, or associated with high-risk occupations (e.g. cash intensive businesses, offshore business, business in high risk countries, online gambling, money-services businesses, trading companies – import/export)

**Person or entity identification examples**

- 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.
- 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.

**Client behavior examples linked to contextual behavior**

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

**Financial transactions in relation to the person/entity profile examples**

- 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.

**Products and services examples**

- 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.

**Change in account activity examples**

- 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.

**Atypical transactional activity examples**

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

**Transactions structured below the reporting / identification requirements examples**

- 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.

**Examples of transactions that involve non-Canadian jurisdictions**

- 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.

**Third party examples**

- Multiple payments which are made to an account by non-account holders.
- A 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.
- 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 is suspicious but refuses or is unable to answer questions related to the account or transactions.

**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
- 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 unfavourable conditions unrelated to his or her health or age
- Transaction involves use and payment of a performance bond resulting in a cross-border payment
- Repeated and unexplained changes in beneficiary
- Same beneficiary for multiple policies where the owner/insured is different
- Relationship between the policy holder and the beneficiary is not clearly established

**Terrorist financing indicators**

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

Additional examples can be found in FINTRAC's Money laundering and terrorist financing indicators - Life insurance companies, brokers and agents on their website: http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/li_mltf-eng.asp .

## Part B – Appointment of a compliance officer

Commented [A1]: Who can be the compliance officer? Typically, a principal or sole proprietor would be the compliance officer but another individual could be appointed. The appointed compliance officer should have a thorough understanding of AML requirements, the practice and the client base to be able to identify risks for the practice. The compliance officer can delegate certain responsibilities such as filing reports with FINTRAC, training etc.

Throughout the program you will see procedures have been assigned to the compliance officer, these can also be assigned to a delegate.

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)
- Notifying Canada Life's MLRO's office immediately of unusual or suspicious transactions involving a Canada Life (or subsidiary) product.
- 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: Stephen Ash

POSITION:
Insurance Broker & Compliance Officer

_____ _____

Compliance officer Date

Appointment approved by:

_____ _____

Principal Date

# Part C – Policies and procedures

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

## Section 1 – Reporting to FINTRAC and related record keeping

There are three types of reports that we may be required to submit to FINTRAC. The three types of reports are:

- Suspicious transaction reporting (Section 1.2)
- Large cash transaction reporting (Section 1.3)
- Terrorist property reporting (Section 1.4)

Details of how to report, information required when reporting and related records that must be retained are found in the sections below.

### 1.1 – Enrolment with FINTRAC's electronic reporting system

The compliance officer will ensure we are enrolled with FINTRAC at the time of reporting 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.

**Commented [A2]:** Throughout the document you will see compliance officer listed as the person responsible to carry out various actions, these accountabilities can also be completed by a delegate.

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

### 1.2 – Suspicious transactions reporting and record keeping policy

**What are suspicious transactions?** –FINTRAC's 'What is a suspicious transaction report?' defines suspicious transactions as financial transactions that we have reasonable grounds to suspect are related to the commission of a **money laundering offence or a terrorist activity financing offence**. This includes **attempted** transactions that we have reasonable grounds to suspect are related to the commission of a money laundering offence or a terrorist activity financing offence.

**Requirement** – We have to report completed or attempted suspicious transactions to FINTRAC **as soon as practicable after completing the measures required to establish reasonable grounds to suspect** that a transaction is related to the commission of a money laundering/terrorist financing offence.

**As soon as practicable** means we have completed the following measures that have allowed us to determine that we have reached the threshold for reasonable grounds to suspect, and therefore **must treat the development and submission of the report as a priority to ensure it is timely**:

- screening for and identifying suspicious transactions;
- assessing the facts and context surrounding the suspicious transaction;
- linking ML/TF indicators to the assessment of the facts and context; and
- explaining the grounds for suspicion in an STR, where we articulate how the relevant facts, context and ML/TF indicators allowed us to reach the grounds for suspicion.

In situations involving time-sensitive information, such as suspected terrorist financing and threats to national security, we are encouraged to expedite the submission of STRs. There is no minimum threshold amount for reporting a suspicious transaction. We must make subsequent reports for additional suspicious transactions and periodically re-assess the client to verify that the level of suspicion has not changed.

If we are in receipt of a production order, by law enforcement, we must perform an assessment of the facts, context, and ML/TF indicators to determine whether there are reasonable grounds to suspect that a particular transaction is related to the commission of ML/TF.

Similarly, if we identify a transaction whereby we have reached reasonable grounds to *believe* that an ML/TF offence has occurred, we must begin an assessment of the related transactions immediately as we have *surpassed* the threshold for reasonable grounds to suspect.

**Procedures** – All employees and associate advisors, if applicable, within this practice are required to bring forward any suspicious transactions to the compliance officer **immediately** once they've completed measures that enable us to determine there are reasonable grounds to suspect.

This will enable the compliance officer to develop and submit the suspicious transaction report to FINTRAC as soon as practicable by ensuring the report is timely and unreasonable priority is not given to other tasks. Any delayed reports, should they occur, require a suitable explanation which the compliance officer must keep a record of. For unusual or suspicious transactions involving a Canada Life (or subsidiary) product, the compliance officer will also refer the information to Canada Life's MLRO's office at (ccamlatfteam@canadalife.com). The compliance officer files all suspicious transaction reports with FINTRAC and informs senior management of all suspicious transaction reports. Copies of the submitted reports are retained in a secure location. These records are retained for at least five years from the date the report was submitted.

**Confidentiality and immunity**

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

Since it's important not to tip the client off that we are submitting a suspicious transaction report, we should not request information from the individual conducting or attempting the transaction if we believe that doing so would alert them that a suspicious transaction report is being filed.

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

**Exception for employees** – There is an exception for employees to report, by paper (instead of electronically), directly with FINTRAC in instances where they do not bring forward their suspicion to the compliance officer. Additional information regarding how to submit paper reports can be found in the Paper Reporting section of the "Reporting suspicious transactions to FINTRAC": http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide3/str-eng.asp.

**Information to be contained in suspicious transaction report**

Consult "Reporting suspicious transactions to FINTRAC": http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide3/str-eng.asp

Complete all applicable fields in the report including a detailed explanation of what led to the suspicion. Only populate non-mandatory fields on suspicious transaction reports. if the information is contained within client files, and if this information was not collected, then, in some cases, you are required to take reasonable measures to attempt to get the information. If there is more than one transaction that contributed to the suspicion, include them in the same report.

If available in our client file, include additional information in Part G to assist FINTRAC in its analysis and production of financial intelligence disclosures, such as nicknames, beneficial ownership information, IP addresses, additional account numbers, email addresses, and relationships.

## 1.3 – 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 and My Par Gift participating 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.** Additionally, we do not

**Commented [A3]: Customization Tip** - If cash is accepted within the practice this statement should be removed and consideration should be given to enhancing policies and procedures in the section of the program.

accept any form of virtual currency and therefore will not be required to report or keep records of certain virtual currency transactions.

**Procedures** –
Clients offering to provide cash for the payment of a 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:

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 – 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.**

**Commented [A4]: Customization Tip** - If cash is accepted within the practice this statement should be removed and consideration should be given to enhancing policies and procedures in the section of the program.

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 and CSIS. Terrorist property reports must be submitted on 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.

### 1.5 – Voluntary self-declaration of non-compliance

**Requirement –** If we come across instances where we have not met all of the requirements of reporting, client identification, record keeping or effectively implementing an area of our compliance program, we must report our non-compliance to FINTRAC without delay.

**Policy** – All instances of non-compliance shall be brought forward to the compliance officer.

**Procedures –** All employees and associate advisors, if applicable, within this practice are required to bring forward any instances of non-compliance to the compliance officer as soon as first suspected. The compliance officer files all voluntary self-declaration of non-compliance reports with FINTRAC and informs senior management of all voluntary non-compliance reports. Copies of the submitted reports and the acknowledgment received in return from FINTRAC are retained in a secure location.

Additional details are available in FINTRAC Voluntary self-declaration of non-compliance: http://www.fintrac-canafe.gc.ca/guidance-directives/exam-examen/vsdonc/1-eng.asp

## Section 2 – 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 and/or funds, intended use of the policy, third party involvement and any known political exposure.

For clients that 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.

### 2.2 – Information record

**Policy** – 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 and My Par Gift participating life insurance policies. Other products are exempt from information record requirements. We do not remit funds to any beneficiaries (this is the responsibility of the insurer) and therefore do not have beneficiary information record or related requirements.

**Procedures** – In practice, we comply with the obligation to create an information record by completing insurer applications for insurance products, which capture all of the required information. Information retained in 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 information records include:

- Client identification information (individuals and entities)
- Industry and occupation (nature of business for entities)
- Beneficial ownership, control and structure information (entities)
- Third party determination and information
- Politically exposed person determination (if $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 information record are outlined in Section 2.3.

## 2.3 – Summary chart

**Commented [A5]:** This section summarizes the client information required to be documented and retained for individuals and entities. This information is required from the insurer and is documented when completing applications and required forms. No customization is required in this section.

| Information record component | When required | Information required to be recorded/retained |
|---|---|---|
| **Information for individual policy holders –** Recorded on applications and forms. | If $10,000 or more is expected to be received over the duration of the annuity or life insurance policy. | **Client information:**<br>• Name<br>• Address<br>• Date of birth<br>• Detailed Industry and occupation<br><br>**Client identification details:**<br>• Identification details (including details of type, identifying number, place of issue, expiry) **see Section 3.1 Identity verification for individuals for details of required information* |
| **Policy holder information and beneficial ownership, control, structure records for entities** – Recorded on applications, forms and copies retained of supporting documentation from the client.<br><br>** See below for definitions and additional policy and procedure information.* | If $10,000 or more is expected to be received over the duration of the annuity or life insurance policy. | **Client information for all types of entities:**<br>• Entity name<br>• Address<br>• Detailed description of the entity's principal business and industry<br>• Incorporation or other identifying number<br>• Jurisdiction of incorporation<br>• For securities only: Signatory information (name, address, DOB, occupation, identification including details of type, identifying number, place of issue, expiry) |

| | | |
|---|---|---|
| | | **Information to verify the identity of an entity and beneficial ownership, structure and control information;**<br>• For all entities: Copies of documents used to verify the identity such as:<br>o Certificate of corporate status, corporate profile report (corporations)<br>o Notice of assessment issued by municipal, provincial, territorial or federal government (corporations)<br>o Partnership agreement (entity other than a corporation)<br>o Articles of association (entity other than a corporation)<br>o Trust agreement (for a legal trust)<br>o Charity registration records on CRA (registered charity)<br><br>**Not-for-profit organization requirements**<br>Determine if the entity is a registered charity for income tax purposes. If it's not a registered charity, determine if it solicits charitable financial donations from the public.<br><br>• For a corporation: Copies of records obtained to confirm the names of all directors (for corporation). The same record can be used to verify the identity of the entity if the information is present (e.g. corporate profile report).<br><br>• For all entities: Copies of records (or an attestation) obtained to confirm information about the individuals who beneficially own or control the entity<br>o Information establishing the ownership, control and structure of the entity, including:<br>➢ Names and addresses of trustees, known beneficiaries and settlors of the trust (for policyowners who are trusts)<br>➢ Names and addresses of all individuals who directly or indirectly own or control 25% or more of the entity (for |

| | | |
|---|---|---|
| | | policyowners that are entities other than trusts)<br>▪ For charities: If it's determined no one person owns and controls 25% directly or indirectly (i.e. the board has more than four members with equal voting rights) - record "none" and provide information about the structure of ownership and control as your confirmation.<br>➢ Organizational chart demonstrating structure.<br><br>• Obtain and retain copies of provisions relating to power to bind such as:<br>o Articles of incorporation/association<br>o Shareholder or partnership agreements<br>o Annual return (T1 Sch50 or equivalent)<br>o Bylaws of the corporation<br>o Certificate of incumbency<br>o Trust deed<br>o Evidence of power to bind<br><br>If this information cannot be obtained or accuracy not confirmed, additional action is required*. |

| | | |
|---|---|---|
| **Third Party Determination and information –** Recorded on applications and forms.<br><br>** See below for definitions and additional policy and procedure information.* | When an information record is kept for the policy holder ($10,000 or more is expected to be received over the duration of the annuity or life insurance policy). | Third party determination – is the client acting on behalf of someone else? Yes or no is recorded on applications and forms.<br><br>If yes, the following is collected;<br><br>• Name and address of third party<br>• Occupation or principal business of third party<br>• Date of birth (if an individual)<br>• Telephone number<br>• Incorporation number and place (jurisdiction) of incorporation<br>• Nature of relationship between third party and client<br><br>If involvement of a third party is suspected even though the client has declared there is not a third party, 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.<br><br>** See below for definitions and additional policy and procedure information.* | For the contributor of deposits $100,000 or greater for an annuity or life insurance policy.<br><br>*Since we do not remit funds to beneficiaries, beneficiary PEP determination requirements are not applicable. Insurers are responsible for these requirements if $100,000 or more is remitted to a beneficiary over the duration of a life insurance policy or annuity.* | • PEP determination – is client a PEP or HIO (includes relatives/close associates)? Yes or no recorded on applications and forms. If yes, we require:<br>• The name, relationship and office/position of the individual who is a PEP and country<br>• The source of the funds, if known, that were used for the transaction<br>• The source of the person's wealth, if known<br>• The date you determined the individual to be a PEP or HIO<br>• The name of the member of senior management who reviewed the transaction and the result of that review (e.g. approval to keep account open for existing business)<br>• The date the transaction was reviewed |

| | | |
|---|---|---|
| **Business relationship information –** Recorded on applications and forms.<br><br>** See below for definitions and additional policy and procedure information.* | When we conduct two or more transactions in which we have to verify ID for a client, 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.).<br><br>Ongoing monitoring of the business relationship according to the level of risk, including:<br><br>• Keeping client information, beneficial ownership, and purpose/nature of business relationship up to date<br>• Detecting any suspicious transactions<br>• Reassessing the level of risk associated with the client's transactions and activities<br>• Determining whether the transactions are consistent with the information and risk assessment for the client. |

## a) Beneficial ownership, control and structure 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** a corporation or other 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. For a trust, the beneficial owners are the trustees and any known beneficiaries or settlors of the trust. **Policy** – When confirming the identity of an entity, we also need to obtain information about the ownership, control and structure of the entity and take reasonable measures to confirm and keep records of the information. This 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.

For additional information on verifying the identity of entities see Section 3.2 Verify the i*dentity of entities* of this program.

**Procedures** – We must search through as many levels of information as necessary in order to determine beneficial ownership. However, there may be cases where we obtain information confirming that there is no individual who owns or controls 25% or more of an entity. We must still keep a record of the information obtained to demonstrate this. In cases where we are able to obtain information and confirm that there is no individual who owns or controls 25% or more of the entity, we do not need to verify the identity of the chief executive officer (or person who performs that function), as this is different than *not being able to* obtain or confirm beneficial ownership.

Reasonable measures must be taken to confirm the accuracy of the beneficial ownership information obtained. These reasonable measures cannot be the same as the measures used to obtain the information. Reasonable measures to confirm the

accuracy of beneficial ownership information could include asking the client to provide suitable documentation (such as an attestation) or referring 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) must be kept in our records.

For complex entities, our reasonable measures must go further in order to ensure we are able to understand and confirm the beneficial ownership, as well as establish the ownership, control and structure of that entity. Additional measures for verifying the ownership, control and structure of complex entities may be included on insurer forms

If you are unable to obtain or confirm this information (or the client refuses), we must:
• take reasonable measures to verify the identity of the CEO or person who performs that function.

• treat the entity's activities as high-risk

• apply enhanced measures for high-risk clients, including enhanced ongoing monitoring.

A decision may also be made not to proceed with doing business with this client without this information. If the client refuses to provide this information, consideration should be given as to whether the transaction (or proposed transaction) is suspicious.

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

## b) Third party determination and records

**Who is a third party?** – A third party is a person or entity who instructs another person or entity to conduct an activity or financial transaction on their behalf. 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. For our purposes, a third party can be an individual or entity, other than the client, who conducts the transaction/financial activity such as a payor, power of attorney, nominee or someone directing the transaction.

**Policy** – We make a third party determination (request the client to disclose if a third party exists) when we are required to keep an 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 as outlined in the chart above.

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 an 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

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

**Who is a PEP?**

| Domestic | Foreign |
|---|---|
| A person who holds, or has held **within the last 5 years**, the following position(s) in or on behalf of a **Canadian** federal, provincial or municipal government:<br><br>• Governor General, lieutenant governor or head of government;<br>• member of the Senate or House of Commons or member of a legislature;<br>• deputy minister or equivalent rank;<br>• ambassador, or attaché or counsellor of an ambassador;<br>• military officer with a rank of general or above;<br>• president of a corporation that is wholly owned directly by Her Majesty in right of Canada or a province;<br>• head of a government agency;<br>• judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;<br>• leader or president of a political party represented in a legislature; or<br>• mayor, reeve or other similar chief officer (or equivalent head of a city, town, village, or rural (country) or metropolitan municipality, regardless of the size of the population). | A person who holds, or has ever **held** , the following position(s) in or on behalf of a **foreign** state:<br><br>• head of state or head of government;<br>• member of the executive council of government or member of a legislature;<br>• deputy minister or equivalent rank;<br>• ambassador, or attaché or counsellor of an ambassador;<br>• military officer with a rank of general or above;<br>• president of a state-owned company or a state-owned bank;<br>• head of a government agency;<br>• judge of a supreme court, constitutional court or other court of last resort; or<br>• leader or president of a political party represented in a legislature. |

**Who is an HIO?**

A person who is **currently holds or has held within the last 5 years** either:

- the head* of an international organization established by the governments of states; or
- the head* of an institution established by an international organization.
- the head* of an international sports organization

*the primary person who leads that organization, for example a president or CEO. An example of an international organization would be NATO, United Nations, UNICEF, etc.

**A PEP (foreign or domestic) or HIO also includes the following relatives and close associates:**

| Family member | Close associate |
|---|---|
| A person with one of the following defined relations to a PEP or HIO:<br><br>• Mother or father (biological and adoptive)<br>• Child (biological and adoptive)<br>• Spouse/common-law partner/civil union/ domestic partner (including ex-spouse)<br>• Parents-in-law (includes those of spouse/common-law partner/civil union/ domestic partner)<br>• Siblings (includes biological, half, and adopted siblings only)<br>  ○ This does not include step-siblings unless they were legally adopted by the PEP/HIO. | A person who is closely connected to a PEP or HIO for personal or business reasons, for example (but not limited to):<br><br>• joint on a policy with a PEP or HIO<br>• business partners with, or who beneficially owns or controls a business with, a PEP or HIO<br>• in a romantic relationship with a PEP or HIO, such as a boyfriend, girlfriend or mistress<br>• involved in financial transactions with a PEP or a HIO<br>• a prominent member of the same political party or union as a PEP or HIO<br>• serving as a member of the same board as a PEP or HIO<br>• closely carrying out charitable works with a PEP or HIO |

**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 individual is a PEP, within the 30 days we also must have the transaction approved by senior management within the practice.

Upon determination that the individual is a PEP or HIO, or relative/close associate (RCA) of such a person, a risk assessment must be performed. If the client is a foreign PEP or RCA to a foreign PEP, then they are immediately considered high risk and treated as such.

If any PEP or HIO is considered high risk as a result of the risk assessment, then the applicable special measures are required to be completed within 30 days of the transaction. These special measures include;

1. Taking reasonable measures to collect the source of funds of the transaction
2. Having the transaction approved by senior management within the practice
3. Recording all of the steps taken for the determination, review and approval

*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/HIO; 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/HIOs.

If the client is a PEP/HIO we:

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

*We have 30 days after the day on which we receive a lump-sum payment of $100,000 or more or detect a fact about existing account holders that indicates a PEP or HIO connection, to take reasonable measures to establish the source of a person's wealth.

**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 subsequent $100,000 lump sum deposit to an insurance policy or annuity, since the individual's status may have changed.

## d) Business relationship record

**What is a business relationship?**

A business relationship is a relationship established between us, as a reporting entity, and a client to conduct financial transactions or provide services related to those transactions.

A business relationship begins the second time, within a 5-year period, that the client engages in a financial transaction for which we are required to verify their identity.

Even in situations where the regulations allow for an exception to verifying a client's identity for the second transaction (e.g. if there are no doubts about the first verification), a business relationship is still created. This is because the underlying requirement to verify a client's identity or confirm the existence of an entity still exists for the second transaction. However, if a **general exception** applies, such as an exempt policy, public body, or very large corporation, then a business relationship is not created for that client as there is no requirement to verify their identity.

**When does the business relationship cease?**
If the client no longer has any active business with us, the business relationship is considered to have ended 5 years after the termination of the last contract.

**Policy** – We must keep a record of the purpose and intended use of any 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.

Reasonable measures must not be confused with, and do not apply to requirements that are mandatory, that is, where information must be obtained before the transaction or activity can be completed (e.g. verification of client identity).

## Section 3 – Identity verification

**Policy** – The identity of individuals and/or entities is verified for non-registered annuities, non-registered investments or universal life and My Par Gift participating 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.

Identification details are recorded on applications and forms.

See *section 3.1 of this program* for measures taken/procedures to verify the ID of individuals and *section 3.2 of this program* for measures taken/procedures to verify the identity of entities.

## 3.1 Verify the identity of individuals

**Procedures** – To verify the identity of an individual, we refer to one of two methods. Either an advisor or a licensed assistant who is contracted with the agency or insurer can verify an individual's identity.

**Single Record Photo ID method**

The document must be authentic, valid and current at the time the individual's identity is verified. For example, an **expired** driver's license would **not** be acceptable.

To authenticate a government-issued photo identification document, review the original of the physical document, not copies, and examine its security features in the presence of the client to satisfy that it is authentic as issued by the competent authority (federal, provincial, territorial government), that it is valid (unaltered, not counterfeit) and current (not expired).

The photo-ID document must indicate the individual's name, have a photo of the individual (both of which must match; and have a unique identifier number.

Examples of acceptable photo-ID documents include:

- Driver's licence
- Passport
- Permanent resident card
- Citizenship card (issued prior to 2012)
- Certificate of Indian status
- Other similar document issued by a provincial, territorial or federal government

A valid foreign passport may also be acceptable, however additional records to confirm that the client meets Canadian residency requirements may be required by the insurer.

When using the photo-ID method, applications and forms are designed to record the following required information:

- The individual's name
- Type of card or document used (e.g. driver's licence)
- The unique identifier number on the document or card
- The issuing jurisdiction and country of the document or card (e.g. Alberta, Canada)
- The expiry date, and issue date if available (if the information appears on the card you must record it)
- The date the information was verified

**Dual Process Method of Identification**

For the dual source method, the advisor is required to review two valid and current pieces of information, each from different reliable sources. The individual does not need to be physically present at the time we confirm their identity using this method.

We may use an original record or another version of the information's original format, such as a fax, photocopy, scan, or electronic image.

It is acceptable to use a fax, photocopy, scan or electronic image of a government-issued photo identification document as a source of information.

Each source of information must be used separately to meet one of the following criteria (two out of three categories must be met in total) and we must make sure all the information matches what was provided by the individual:

- Name and address
    - Examples: government-issued photo-ID, utility bill or municipality tax statement or CRA notice of assessment, most recent financial statement from a securities dealer or other investment firm (not our own or from the same insurer)
- Name and date of birth
    - Examples: government-issued photo-ID, marriage certificate or birth certificate (if no name change)
- Name and financial account (i.e. must be a Canadian deposit, credit card, or loan account)

Examples: Most recent credit card bill or savings/chequing account statement from a bank, or loan/mortgage statement (not from the same issurer)

We cannot use the same information or source to satisfy more than one of the categories above. For example, we cannot use a credit card statement to confirm the name and address and again to confirm the name and financial account.

Examples of unacceptable identification information:

- Birth or baptismal certificate issued by a church
- Identification card issued by an employer for an employee
- Health card (unless permitted by provincial legislation)

When using the dual process method, applications and forms are designed to record the following required information:

- The individual's name
- The name of the two different sources of information that were used (for example, Canada Revenue Agency, CIBC)
- The type of information (for example, utility statement, bank statement, marriage license, notice of assessment)
- The account or reference number associated with the information
- The date associated with the information and/or expiry date (to demonstrate the information is current, particularly when a copy of a photo-ID is used)
- The date the information was verified.

If we are unable to obtain identification through the sources listed above we consult FINTRAC's Guidance - Know your client - entities for additional options.

## 3.2 Verify the identity of entities

**Procedures** – Entities include corporations, trusts (including widely-held trusts), partnerships, funds and unincorporated associations or organizations.

To verify the identify of a corporation refer to the following documents to confirm the entity's name and address:

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

To verify the identity of an entity other than a corporation, we refer to a partnership or trust agreement, articles of association or any other similar record that identifies the entity and confirms its name and address match.

The record we use to verify the identity of an entity 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), is not acceptable as we have to refer to a record.

When verifying the identity of a corporation, we also must confirm the names of the directors by referring to a record. This can often be completed using the same document as above, such as a corporate profile record, but in some cases another record may be required.

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), or the Quebec Enterprise Register (http://www.registreentreprises.gouv.qc.ca/en/). A corporation searching and registration service is also acceptable.

## 3.3 Exceptions to client identification

**Policy** – Once the identity of an individual has been verified as noted above we do not have to verify their identity again if we recognize the individual (visually or by voice using caller authentication) and there are no doubts about the information. If there are any doubts or missing information, we verify 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 (https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng ).

Once inherent risks have been identified, we create risk-reduction measures and key controls, and implement that risk-based approach as part of our day-to-day activities.

**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 and business relationships
- New developments and technologies
- 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 verify the identity of clients and ensure they are not acting on behalf of a third party. This method can be used to obscure the true identity of a client or beneficial owner.

**Commented [A6]:** It's important to note that there is no prescribed method for the assessment of risks. What follows is a SAMPLE assessment process which can be adapted or modified to reflect to your business.
FINTRAC's Guidance - Compliance program - Risk-based approach workbook for life insurance companies, brokers and agents

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

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

**New developments and Technologies**
Implementation of new technologies such as mobile payment services and certain methods of non-face-to-face communication could subject the business to a wide range of vulnerabilities that can be exploited for ML. If we intend to put in place a new service/activity/location or introduce a new technology, we must assess it to determine the potential ML/TF risks it may bring to the business, **before it is implemented.**

**Other factors**
Factors such as legal risks and the operational structure of our business model (i.e., number of employees, employee turnover, number of branches etc.) and the impact of new technology in the industry and our business operations are also considered.

Ministerial directives, transaction restrictions, operational briefs and alerts received from subscribing to FINTRAC's mailing list, insurer communications and reviewing 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.

**Commented [A7]:** To subscribe: A pre-filled e-mail will appear on your screen by clicking on "SUBSCRIBE".

Additional resources can be found on FINTRAC's website in Guidance - Compliance program – Risk Assessment Guidance.-

**How individual clients are risk assessed (initially and ongoing)**

**Commented [A8]:** This is a SAMPLE process to risk assess clients. Other processes are acceptable. Processes should be able to demonstrate that you have assigned the correct risk category to clients.

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, or terrorist property report has been filed
- A client who is an identified terrorist
- A client for whom we are unable to obtain or confirm beneficial ownership information at onboarding or through ongoing monitoring (updating of information).
- A client with transactions sent to or received from a high risk country (e.g. Iran) 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, or where we are not able to collect third party information.
- Occupation – High-risk occupations (e.g. cash intensive businesses, off shore business, business in high risk countries, online gambling, money-services businesses, trading companies – import/export)
- Client's business structure or transactions seems unusually complex
- Non face-to-face client identification without justifiable reason
- Involvement of gatekeepers (i.e. accountants/lawyers) without justifiable reason

**Geography**:

- Client resides outside local or normal customer area
- Client resides in known high-crime area
- Client has off-shore business activities or owns apparent shell companies/holding companies in known tax havens
- Client transactions/connections to high-risk countries (e.g. Iran)

**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.

**Commented [A9]:** This is a SAMPLE method to document and record your assessment of high or potentially high-risk clients. Other methods are acceptable such as client file coding, spreadsheets, notes etc. Legislation requires you to be able to demonstrate the client was assigned the correct risk category.

If you are using an alternate process replace this section and the appendix with details of your process.

## 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.

Regardless of the frequency that a factor may be present, (i.e. some products sold rarely or never), risk mitigation measures have been developed and will be followed if the situation occurs.

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

Once a business relationship is established, we must conduct ongoing monitoring of all clients to:

- Detect suspicious transactions that have to be reported
- Keep client identification information, beneficial ownership information, and the purpose and intended nature of the business relationship record up-to-date
- 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

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

- The individual's name
- Address
- Occupation or principal business
- Confirm that the purpose of the policy/business relationship is still accurate as changes may explain changes in transactional behavior (e.g. frequent withdrawals).

For entities confirm/update the following information:

- Name
- Address
- Nature of business
- Name of directors, trustees etc.
- Beneficial ownership information (Information on the individuals who ultimately control the entity)
- Confirm that the purpose of the policy/business relationship is still accurate as changes may explain changes in transactional behavior (e.g. frequent withdrawals).

**Frequency** – The frequency with which we conduct ongoing monitoring of business relationships and update client information depends on the client's risk rating, with high-risk clients being monitored/updated more frequently. Client information for all clients is also updated periodically via the process to complete a new application for a non-registered investments and annuities, Universal Life insurance policy and to some extent whole life which is exempt under s. 306 (1) of the Income Tax Regulations by the insurer (PCMLTFR s. 154 (2)(a)).

**Low-risk clients** – Transactions are monitored/reviewed/assessed when they are conducted.

Client information for low risk clients is kept up-to-date by verbally confirming information with clients during ongoing interactions new business and periodically with subsequent transactions, if any, at least once every five years.

**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 information for high risk clients is updated annually. Information can be verbally confirmed with the client. Enhanced measures may include:

**Commented [A10]:** This is a SAMPLE method to meet your obligations. The guidelines state that a record of how you do ongoing monitoring should be retained. If you carry out alternate procedures add details in this section.

- taking reasonable measures to confirm information provided by high-risk clients by conducting internet searches
- obtaining additional information on the source of funds/wealth of the client
- obtaining information about the reasons or purpose for certain transactions
- taking additional steps to verify documents or information provided by the client

## 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**<br><br>***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**<br><br>***Assess each factor as high or low.*** | **RATIONALE**<br><br>***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 (segregated funds) | HIGH | Ability to accumulate investments, ease of withdrawals and transfers, ability for third parties to transact using the product. | Cash is not accepted; would be less likely to be exposed to the placement stage of money laundering.<br><br>Obtain source of funds for all clients.<br><br>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 investments, ease of withdrawals and transfers, ability for third parties to transact using the product, transfer of ownership, ability to over pay | Cash is not accepted; would be less likely to be exposed to the placement stage of money laundering.<br><br>Obtain source of funds for all clients.<br><br>Training for employees to ensure an understanding of the products that we sell |

**Commented [A11]:** A list of risks and a typical risk rating have been provided in this column. Inherent risk ratings provided do not need to be customized as they reflect FINTRAC ratings.

The list of risks provided may not reflect all risks applicable to all practices. Add additional risks as necessary to take into account all of your products, services and delivery channels, geography and other relevant factors that may affect your business.

For more examples on how to risk assess see FINTRAC's Guidance on The Risk Based Approach.

**Commented [A12]:** These are SAMPLE risk mitigation measures that can be implemented to meet your obligations. If these can be carried out in your practice no customization is necessary. However, additional measures can be added to reflect additional/alternate procedures carried out in your practice.

| | | | |
|---|---|---|---|
| | | | and the risk of ML/TF that is present with these products and related transactions. |
| My Par Gift participating life insurance policy | High | Ability to over pay and withdraw funds.<br>Third-party is always involved (paying or directing the charity to apply).<br>Policyowner is always a charity (charities are more vulnerable/higher risk for money laundering and terrorist financing). | Cash is not accepted; would be less likely to be exposed to the placement stage of money laundering.<br><br>Obtain source of funds for all clients.<br><br>Charity is registered with the CRA.<br><br>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 (tax exempt policies only) | LOW | Exempt product subject to tax-exempt rules.<br>Ability for third parties to transact using the product, transfer of ownership, ability to over pay and withdraw funds. | Not required as risk assessed as LOW |
| Term | LOW | Exempt product. No build up of cash value, no ability to withdraw or repayment of contributions. Ability for third parties to transact using the product, transfer of ownership. | Not required as risk assessed as LOW |
| Group insurance | LOW | No cash surrender value or saving component. | Not required as risk assessed as LOW |
| Registered investments/annuities | LOW | Exempt product. | Not required as risk assessed as LOW |
| **Delivery channels** | | | |
| Face to face (on-boarding and ongoing transactions) | LOW | | Not required as risk assessed as LOW |
| Non face-to-face delivery channels (telephone, email, Skype, etc.) | 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 a transaction requiring ID (business relationship).<br><br>Not accept new client if they are unwilling to meet face to face without a 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. | 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. | 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.<br><br>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 be less likely to be the first point of entry.<br><br>Obtain source of funds for all clients. |
| Business conducted in geographic location(s) known to have **low presence of crime**? | LOW | Low presence of crime reduces the risk that source of funds may be from illegal activities. | Not required as risk assessed as LOW |
| Business conducted in geographic location(s) known to have **high presence of crime**? | HIGH | Areas with higher crime may have clients with sources of funds from criminal activities. | Obtain source of funds for all clients.<br><br>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.<br><br>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? | 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? | 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.<br><br>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, or source of funds originating from foreign countries that potentially pose a risk of ML/TF? | HIGH | Transactions from foreign jurisdictions are potentially a higher risk for ML/TF. | Obtain source of funds for all clients.<br><br>Reassess the level of risk associated with the client as transactions occur.<br><br>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 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". |
| **New developments and technologies** | | | |
| Use of higher risk payment methods such as:<br>- e-wallets and mobile payments in fiat currency (ApplePay, PayPal in CAD, USD)<br>- e-wallets in virtual currency (Bitcoin)<br>- pre-paid cards<br>- money transfers between individuals over mobile devices or internet (e.g. email money transfer) | HIGH | These payment methods can be used to transfer funds faster and anonymously, which can increase ML/TF risks. | We do not accept payments from clients through any of these higher risk payment methods. |
| Methods of communication or identification that rely on technology, such as:<br>- document signing over server (DocuSign)<br>- online/virtual platforms (Skype, Zoom) | LOW | The increasing use of technology for communication and verification may allow the client to conduct more transactions in a non-face-to-face manner or to obscure their identity/use of third parties. | No new technologies are used to conduct business or contact clients.<br><br>We ensure that our clients are who they say they are and conduct third party determinations as required.<br><br>Security protocols are in place to protect customer information.<br><br>We ensure the customer is authenticated appropriately before any transaction is |

| | | | |
|---|---|---|---|
| - chat applications (WhatsApp, Facebook Messenger)<br>- electronic information exchange<br>- digital ID verification software | | | conducted through DocuSign or any online/virtual platform.<br><br>We do not share any personal details or conduct transactions via external chat applications with clients.<br><br>We do not use Digital ID verification software. |
| New business developments such as:<br>- acquisitions<br>- changes to business model<br>- business restructuring | LOW | New acquisitions and changes to the business model can expose the practice to new products, clients, and geography risk.<br><br>Acquisitions also may increase the risk of non-compliance if the AML/ATF program of the entity is insufficient/ineffective. | We review the effectiveness of the compliance program, as well as the book of business, prior to any new acquisitions.<br><br>Before changing the business model or restructuring, we assess the risk of any new customers, geography, products/services, or other risks to ensure they are in line with our risk tolerance.<br><br>We do not engage in new business developments without the approval of our Compliance Officer. |
| **Other risk factors** | | | |
| Business model - established practice, trained employees, low employee turnover and consistent geographic location | LOW | Characteristics such as low number of employees and/or low employee turnover,<br>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. | 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.<br><br>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 verify 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 funds, purpose of the policy etc., that do not have any automatic high-risk triggers. | N/A | N/A |
| **Group B – HIGH** | Clients for whom suspicious transaction reports have been previously submitted as reasonable grounds for suspicion have already been established.<br><br>Politically Exposed Foreign Persons (PEFP) or Domestic PEP/HIO assessed as high risk, as they may be vulnerable to ML/TF or corruption due to their position, relationship or influence.<br><br>Clients for whom we are unable to obtain beneficial ownership information. This may indicate that the client is trying to hide the beneficial owner.<br><br>A client that is an identified terrorist or suspected to be involved in terrorist activities<br><br>A client with transactions sent to or received from North Korea or Iran (regardless of amount)<br><br>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 | **Enhanced ID measures**<br><br>Ensure ID is verified at time of application with a valid piece of photo identification issued by a federal or provincial government. | **Mitigation measures may include:**<br><br>• Completion of the *Client risk assessment tool (see appendix)* documenting rationale for assessment.<br>• Perform an internet search of the client to see if there is any adverse media.<br><br>**Keeping information up-to-date:**<br><br>• Confirm/update client identification information with the client at every transaction and perform subsequent online searches.<br><br>**Enhanced ongoing monitoring**<br>• Review each transaction made by high risk clients at the time the transaction is conducted.<br>  ○ Maintain notes detailing the review of client transactions. |

**Commented [A13]:** All factors assessed as high risk require enhanced measures to verify/ascertain ID. SAMPLE measures have been provided.

**Commented [A14]:** All groups assessed as high risk MUST have **risk mitigation, enhanced monitoring and processes to keep information up-to-date.**

SAMPLE procedures are provided. The SAMPLE procedures are not meant to be an exhaustive list Add additional risk mitigation measures if needed to reflect your practice.

**Commented [A15]:** You can create as many groupings as you feel are necessary for your client base. Other groupings may reflect clients that you determine to be moderate risk, or further refining your high-risk grouping by specific client characteristics.

**Commented [A16]:** Actions listed below are SAMPLES of enhanced ongoing monitoring procedures that can be carried out to meet your obligations. This list can be customized to reflect how you will carry out ongoing monitoring in your practice.

| | | | |
|---|---|---|---|
| | listed in the risk assessment tool – See appendix. | | ○ Compare the transaction to the purpose and nature of the business relationship.<br>○ Evaluate transaction against the client's profile.<br>○ Request additional information from client if transaction seems inconsistent with client profile.<br>• Periodic review of client transactions<br>• Where STR submitted, annual re-assessment conducted and documented |

## Section 5 – Timeframe for keeping records

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

- Information records (including individual client identification)
- Records to verify the identity 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.

**These records must be kept in such a way that they can be provided within 30 days upon request.**

## Part D – Ongoing training program

Ongoing training is mandatory for 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 for existing staff if needed based on changes to legislation, new products, changes in services offered, geography, technologies, or delivery channels.

**Method** – Training is completed through circulation and review of Sections A and C of our compliance program.

Section A - contains AML/ATF background information as related to our business including definitions, suspicious transaction indicators, reasons to suspect suspicious activities and our responsibilities.

Section C – Policies and procedures includes details for detecting ML/TF, including identification, know-your-client, record keeping responsibilities and our reporting process.

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.

**Commented [A17]:** Circulation of the policies and procedures and background section is a SUGGESTED method to meet training obligations however the method may vary depending on the nature, size of your practice, number of employees etc.

Remove this method and replace with an alternate method if your practice will meet training obligations in another method.

**Commented [A18]:** Be sure to document on the next page that all employees have received training as evidence you have met your training obligations.

### Training completion tracking

**Commented [A19]:** Record training delivered on this tracking sheet. Have employees sign to indicate they received training.

| 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, 2022* | |
| | | | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 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: _____

**Commented [A20]:** Record the date your practice adopted this program.

# 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;<br><br>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:<br><br>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 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. |

**Commented [A21]:** This review can be completed by another employee or an outside consultant/auditor if feasible.

**Commented [A22]:** SAMPLE responses have been provided as a demonstration of how to complete this column. Comments here should reflect the results of your testing. Ensure that you have completed the test steps and that the sample responses are appropriate based on your review. **NOTE more than one sample response has been included for some of the test steps, be sure to customize to reflect your response.**

| | | |
|---|---|---|
| | Yes | We retain a copy of appropriate records related to any reports submitted 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, new developments/technologies, and other factors) and that the assessments accurately reflect your current business and client base. | Yes | Risk assessments include all categories. |
| 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<br><br>NA | Reviewed 10% of high risk clients, evidence of periodic review was noted.<br>OR<br>At this time there are no high risk clients identified in the practice |
| g) Confirm enrolment to receive FINTRAC's operational briefs and alerts for more information on ML/TF. | Yes | We are enrolled to receive FINTRAC's operational briefs and alerts. |
| **3) STRs are documented and submitted according to our processes.** | | |
| a) Review submitted STRs to determine if similar unreported scenarios exist in book of business. | NA<br><br>Yes | We do not have STRs at this time.<br><br>There are no unreported STRs. |
| b) Review submitted STRS to ensure periodic re-assessment conducted and documented. | NA<br><br>Yes | We do not have STRs at this time.<br><br>Periodic re-assessments were conducted and documented as per our procedures |
| c) Review submitted STRS to ensure all fields populated where information was known. | NA<br><br>Yes | We do not have STRs at this time.<br><br>STR fields were completed with the known information. |

| | | |
|---|---|---|
| d) Review measures taken for STRs to reach Reasonable Grounds to Suspect (facts, context and ML/TF indicators) and when these measures were completed (compared to previously submitted transactions, and the complexity, number and nature of the transaction) to ensure the STR was reported as soon as practicable once we met the RGS threshold. | NA<br><br>Yes | We do not have STRs at this time.<br><br>STRs were submitted as soon as practicable. |
| **4)Program review has been completed at least every two years and results reviewed** | | |
| Testing includes:<br><br>a)Confirm that a program review has been completed within the past two years | N/A<br><br>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.<br><br>OR<br><br>This program is the first program documented for the practice, a self review will be completed within two years.<br><br>OR<br><br>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. |
| **5)Ongoing compliance training –** policies and procedures for the frequency and method of training are in place and effective | | |
| Testing includes:<br><br>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** | | |

Commented [A23]: Document any changes that need to be implemented as a result of the review.

## Part G – Revision history

Commented [A24]: Retain prior versions of your programs to demonstrate continuity. Record changes to this program here when/if you make changes.

| Date | Section changed | Reason for change |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

# Appendix

## Client risk assessment tool

Commented [A25]: This is a SAMPLE method to document and record your assessment of high or potentially high risk clients. Other methods are acceptable such as client file coding, spreadsheets, notes etc. Legislation requires you to be able to demonstrate the client was assigned the correct risk category.

Delete this section and references to it in Section 4.1 if an alternate method to document high-risk clients is used.

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 (e.g. cash intensive businesses, off shore business, business in high risk countries, online gambling, money-services business, trading companies – import/export)
- Client's business structure or transactions seems unusually complex
- Non face-to-face client identification without justifiable reason
- Involvement of Gatekeepers (i.e. accountants/lawyers) without justifiable reason

**Geography**:

- Client resides outside local or normal customer area
- Client resides in known crime area
- Client has off-shore business activities, or owns apparent shell companies/holding companies in known tax havens
- Client transactions/connections to high-risk countries (e.g. Iran)

**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.**