COMPLIANCE PROGRAM FOR ANTI-MONEY LAUNDERING AND TERRORISM FINANCING

~~Advisor name/Corporation name~~SHEBA Distributors Ltd. O/A SARKISSIAN Financial Group | AccuTAX Plus
(the practice)

Compliance officer: Bedros SARKISSIAN

Date program adopted: January 2011
Revised on: January 2017

Table of contents

Part A – Background information

Commented [MM1]: This section includes information in addition to policies and procedures that is legislatively required to be covered in training. A review of this section in conjunction with a review of policies and procedures can help meet your training obligations.

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

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

i) What is money laundering?

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

There are three stages in the money laundering process:

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

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

Methods of money laundering

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

reporting. Examples of flags to be aware of and transactions which could be connected to money laundering are provided in section v) below.

ii) What is terrorist financing?

Under Canadian law, terrorist activity financing is when you knowingly collect or provide property, such as funds, either directly or indirectly, to terrorists. The main objective of terrorist activity is to intimidate a population or compel a government to do something. Terrorists need financial support to carry out terrorist activities and achieve their goals. Many of the techniques used to perform money laundering are also used within terrorist financing, including, but not limited to obscuring the direction of funds and the use of third parties. They need to disguise their money as coming from another source, and put it into a form that cannot be easily traced so that it is useable.

Methods of terrorist financing

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

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

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

iii) Our responsibilities

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

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

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

- Appointment of a compliance officer
- The development and application of written compliance policies and procedures

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

iv) Penalties for non-compliance

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

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

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

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

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

Criminal penalties may include the following:

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

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

v) Indicators of suspicious transactions or potential high-risk clients

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

General indicators

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

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

Industry specific examples

- Client wants to use cash for a large transaction
- Client proposes to purchase an insurance product using a cheque drawn on an account other than his or her personal account
- Client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment
- Client who has other small policies or transactions based on a regular payment structure makes a sudden request to purchase a substantial policy with a lump sum payment
- Client conducts a transaction that results in a conspicuous increase in investment contributions
- Scale of investment in insurance products is inconsistent with the client's economic profile
- Unanticipated/inconsistent modification of client's contractual conditions, including significant or regular premium top-ups
- Unforeseen deposit of funds or abrupt withdrawal of funds

- Involvement of one or more third parties in paying the premiums or in any other matters involving the policy
- Overpayment of a policy premium with a subsequent request to refund the surplus to a third party
- Funds used to pay policy premiums or deposits originate from different sources
- Use of life insurance product in a way that resembles use of a bank account, namely making additional premium payments and frequent partial redemptions
- Client cancels investment or insurance soon after purchase
- Early redemption takes place in the absence of a reasonable explanation or in a significantly uneconomic manner
- Client shows more interest in the cancellation or surrender of an insurance contract than in the long-term results of investments or the costs associated with termination of the contract
- Client makes payments with small denomination notes, uncommonly wrapped, with postal money orders or with similar means of payment
- The duration of the life insurance contract is less than three years
- The first (or single) premium is paid from a bank account outside the country
- Client accepts very 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
- Relationship between the policy holder and the beneficiary is not clearly established

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

Part B – Appointment of a compliance officer

The compliance officer is responsible for:

- The implementation, monitoring and updating of the compliance program which includes:
  - Policies and procedures for reporting, record keeping, client identification, risk assessment and risk mitigation
  - Risk-based approach
  - Training
  - Program evaluation
- Making necessary reports to FINTRAC (suspicious transactions, large cash transaction, terrorist property reports)
- Reporting on a regular basis to the board of directors/senior management/owner

The compliance officer

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

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

NAME: Bedros SARKISSIAN

POSITION: Agency Principal

Digitally Signed: Bedros SARKISSIAN

2018-01-01

Compliance officer Date

Appointment approved by:

SHEBA Distributors Ltd.

2018-0101

Principal Date

Commented [MM2]: 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.

Formatted: Font: Italic

Formatted: Font: Italic, Underline

Formatted: Font: Italic

Formatted: Font: Italic, Underline

Formatted: Font: Italic, Underline

Formatted: Font: Italic, Underline

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, ascertaining identity, risk based approach, and training program.

Section 1 – Reporting to FINTRAC and related record keeping

There are three types of reports that may be required to be submitted 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 is required to ensure we are enrolled with FINTRAC's electronic reporting system, F2R system, to report electronically. Once enrolled, FINTRAC provides an identifier number to include in our reports. This number is retained by the compliance officer. The compliance officer submits all reports to FINTRAC.

Commented [MM3]: 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 guideline 2 defines suspicious transactions as financial transactions that you 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 you 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 **within 30 calendar days of first detecting a fact about a transaction that**

causes reasonable grounds to suspect the transaction is related to the commission of a money laundering offence. There is no minimum threshold amount for reporting a suspicious transaction.

Procedures – All employees and associate advisors, if applicable, within this practice are required to bring forward any suspicious transactions to the compliance officer as soon as first suspected. The compliance officer files all suspicious transaction reports with FINTRAC and informs senior management of all suspicious transaction reports. Copies of the reports submitted and the acknowledgement received in return from FINTRAC are retained in a secure location.

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

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

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

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 FINTRAC Guideline 3B *Submitting suspicious transaction reports to FINTRAC by paper*.

Information to be contained in suspicious transaction report

Consult FINTRAC Guideline 3A *Submitting suspicious transaction reports to FINTRAC electronically*.

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

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 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.

Commented [MM4]: 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.

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

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

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 [MM5]: 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. Terrorist reports must be submitted by paper to FINTRAC. Forms are available as follows:

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

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

Section 2 – Client information record keeping

2.1 – General

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

Individual client information collected may include as required, but is not limited to, their identification, occupation, industry, employment, address, tax residency, date of birth, source of wealth, intended use of the policy, third party involvement and any known political exposure.

For clients which are legal entities, additional information is required which provides the information on the beneficial owners of the entity and those who control the entity, as specified in FINTRAC guidance and outlined below.

2.2 – Client information record

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

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

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

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

2.3 – Summary chart

Commented [MM6]: 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.

Client information record component	When required	Information required to be recorded/retained
Client information for individuals – Recorded on applications and forms.	If the client is expected to pay $10,000 or more for an annuity or a life insurance policy.	**Client information:** • Name • Address • Date of birth • Industry and occupation (descriptive) **Client identification details:** • Identification details (including details of type, identifying number, place of issue, expiry) **see Section 3 Client identity for details of required information*
Client information and beneficial ownership and control records for entities – Recorded on applications, forms and copies retained of supporting documentation from the client. ** See below for definitions and additional policy and procedure information.*	If the client is expected to pay $10,000 or more for an annuity or a life insurance policy.	**Client information for all types of entities:** • Entity name • Address • Incorporation or other identifying number • Jurisdiction of incorporation • Detailed description of the entity's principal business and industry • Signatory information (name, address, DOB, occupation, identification [including details of type, identifying number, place of issue, expiry]) **Information to confirm existence of an entity and beneficial ownership, structure and control information;** • Copies of documents used to confirm existence such as: ○ Certificate of corporate status (corporations) ○ Notice of assessment issued by municipal, provincial, territorial or federal government (corporations) ○ Partnership agreement (entity other than a corporation) ○ Articles of association (entity other than a corporation) • Copies of records obtained to confirm information about the individuals who ultimately control the entity, ownership and provisions relating to power to bind such as:

		○ Articles of incorporation/association ○ Shareholder or partnership agreements ○ Annual return (T1 Sch50 or equivalent) ○ Bylaws of the corporation ○ Certificate of incumbency ○ Trust deed ○ Evidence of power to bind • Names of all directors (for corporations) • Names and addresses of trustees, known beneficiaries and settlors of the trust (for trusts) • Names and addresses of all individuals/entities who directly or indirectly own or control 25% or more of the entity (for entities other than trusts) • Information establishing the ownership, control and structure of the entity. If this information cannot be obtained or accuracy not confirmed record: • Name of the most senior managing officer of the entity and ascertain their identity and treat the client as high risk **Not-for-profit organization requirements** Determine whether or not the entity is a registered charity for income tax purposes. If it's not a registered charity, determine whether or not it solicits charitable financial donations from the public.
Third Party information determination – Recorded on applications and forms. ** See below for definitions and additional policy and procedure information.*	If the client is expected to pay $10,000 or more for an annuity or a life insurance policy.	• Third party determination – is there a third party involved with interest or control of the policy? Yes or no is recorded on applications and forms. If yes, the following is collected; • Name and address of third party • Occupation or principal business of third party • Date of birth (if an individual) • Incorporation number and place of incorporation (if a corporation) • Nature of relationship between third party and client If involvement of a third party is suspected even though the client has declared there is not a third party involved, document why we

		suspect the individual is acting on a third party's instructions
Politically exposed person (PEP) or Head of an International organization (HIO) determination – Recorded on applications and forms. ** See below for definitions and additional policy and procedure information.*	For the contributor of deposits $100,000 or greater for life insurance.	• PEP determination – is client a PEP or HIO (includes close relatives/close associates)? Yes or no recorded on applications and forms. If yes; • The name, relationship and office/position of the individual who is a PEP and country • The source of the funds, if known, that were used for the transaction • The date you determined the individual to be a PEP or HIO • The name of the member of senior management who reviewed the transaction • The date the transaction was reviewed
Business relationship information – Recorded on applications and forms. ** See below for definitions and additional policy and procedure information.*	When we conduct two or more transactions in which we have to ascertain ID or confirm existence of an entity we have entered into a business relationship with the client.	Record of the purpose and intended nature of the business relationship on applications and forms (e.g., financial planning, estate planning, capital preservation etc.).

a) Beneficial ownership and control records

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

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

For additional information on confirming the existence of entities see Client identification Section 3 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 there is no individual who owns or controls 25 per cent or more of an entity. We must still keep a record of the information obtained.

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

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

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

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

b) Third party determination and records

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

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

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

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

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

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

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

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

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

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

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

Terms and expiry

Foreign persons – if the person holds or has ever held (includes deceased)

Domestic persons – if the person holds or has held the position in the past five years

Heads of international Organizations – if the person currently holds the role

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

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

These special measures to be completed within 30 days include;

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

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

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

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

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

d) Business relationship record

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

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

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

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

2.4 – Reasonable measures

Keep a record of any “reasonable measures” you have taken

What are reasonable measures?

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

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

Documenting reasonable measures

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

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

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

Section 3 – Ascertaining client identity

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

Client identification details are recorded on applications and forms.

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

3.1 Individuals

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

Single Record Photo ID method

The original, not copies, of the individual's photo identification is required to be reviewed in the presence if the client and a visual comparison performed:

- 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 with all of the following elements: photo, name, address, date of birth and expiry date.

The document also has to be a valid one and **cannot have expired**. For example, an expired driver's license would not be acceptable.

Dual Record Method of Identification

For the dual record method, original records are required to be reviewed by the advisor from two different reliable sources, which must meet two of the following criteria:

- Name and Address
    - Examples: Utility Bill or Municipality tax statement or CRA notice of assessment
- Name and Date of Birth
    - Examples: Marriage Certificate or Birth Certificate (if no name change)
- Name and Financial Account

- Examples: The most recent financial statement from a securities dealer (not your own firm) or bank account statement

Examples of unacceptable identification documentation:

- Birth or baptismal certificate issued by a church
- Identification card issued by an employer for an employee

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

If we are unable to obtain identification through documents listed above we consult FINTRAC's Guidance - Know your client - Methods to identify individuals and confirm the existence of entities for additional options.

3.2 Confirming the existence of entities

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

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

- The corporation's certificate of corporate status
- A record that has to be filed annually under provincial securities legislation
- Any other record that confirms the corporation's existence. 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 confirm the existence of an entity other than a corporation, refer to a partnership agreement, articles of association or any other similar record that confirms the entity's existence.

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

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

3.3 Exceptions to client identification

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

Section 4 – Risk based approach

4.1 – Risk assessment

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

Commented [MM7]: 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

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

Commented [MM8]: Certain risk categories are expected to be covered in risk assessments. An understanding of these categories is required to complete your risk assessments in the following sections.

The following categories are considered in the risk assessments:

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

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

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

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

- Proximity to an area known for high crime rates is considered
- Client connections to high-risk countries

- Size/nature of area where client base reside i.e., small rural area where clients are known vs. large urban area where clients are unknown

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

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

Commented [L9]: 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 - Guidance on the risk-based approach to combatting money laundering and terrorist financing.

How individual clients are risk assessed (initially and ongoing)

Commented [MM10]: 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, terrorist financing report has been filed
- A client who is an identified terrorist
- A client for whom we are unable to obtain beneficial ownership information
- A client with transactions sent to or received from North Korea (regardless of amount)

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

Client characteristics, product, service, delivery channel:

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

Geography:

- Client resides outside local or normal customer area

- Client resides in known crime area
- Client has off-shore business activities, client connections to high-risk countries

Other suspicious transaction indicators:

- Volume/timing/complexity of transactions inconsistent with purpose of the policy/account
- Value of deposits inconsistent with occupation or source of funds
- Presence of any suspicious transaction 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 [MM11]: 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.

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

Once a business relationship is established we must:

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

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

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

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

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

For entities confirm/update the following information:

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

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

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

Client information can be kept up-to-date by verbally confirming information with clients periodically during ongoing interactions (i.e., new business or subsequent transactions).

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

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

Commented [MM12]: 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.

4.4 – Business based risk assessment

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

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

Commented [MM13]: 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 [MM14]: 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.

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

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

Business conducted in geographic location(s) known to have **high presence of crime**? ___ Frequently ___ Occasionally ___ Rarely/Never	HIGH	Areas with higher crime may have clients with sources of funds from criminal activities.	Obtain source of funds for all clients. On a regular basis information available online regarding crime in our area is reviewed. Sources such as Statistics Canada provide information on crime in Canada by type and region. As necessary training is provided to employees to ensure they are aware of the types of crime in our area and remind them of due diligence at on-boarding such as occupation and source of funds.
Business conducted in smaller city where clients are often known at time of on-boarding? ___ Frequently ___ Occasionally ___ Rarely/Never	LOW	This practice operates in a smaller city and/or clients are often known at time of on-boarding?	Not required as risk assessed as LOW
Business conducted in a large city where new clients are typically unknown to the practice at the time of on-boarding? ___ Frequently ___ Occasionally ___ Rarely/Never	HIGH	In a larger city there is potentially more new client anonymity where clients are often unknown to the practice at time of on-boarding.	Obtain source of funds for all clients. Ensure that we meet in person with all clients before entering into a business relationship.
Are there **connections to high-risk countries**, i.e., wire transfers received from foreign countries that potentially pose a risk of ML/TF? Frequency of occurrence in this practice ___ Frequently ___ Occasionally ___ Rarely/Never	HIGH	Transactions such as wire transfers from foreign jurisdictions are potentially a higher risk for ML/TF.	Obtain source of funds for all clients. Reassess the level of risk associated with the client as transactions occur. Review the sanctioned countries listing annually or as notified of updates to the listing through FINTRAC and/or insurer communications to ensure awareness of high-risk countries. These are available on the Office of the Superintendent of Financial Institutions' website (http://www.osfi-bsif.gc.ca), by referring to the "Terrorist Listings and Sanctions" link.
Other risk factors			
Business model - established practice, trained employees, low employee turnover and consistent geographic location	LOW	Characteristics such as low number of employees and/or low employee turnover, one office location	Not required as risk assessed as LOW

___ Reflects my current practice ___ Does not reflect my current practice		with little anticipated change in geography, products or client base.	
Business model - Larger practices with several employees and/or high turnover that impacts training requirements and practices that may be experiencing changes to their location of client bases may be at an increased risk. ___ Reflects my current practice ___ Does not reflect my current practice	HIGH	This practice has some higher risk factors such as: several employees, different roles, different training needs, several office locations or anticipated changes to geography, products and/or client base.	Ensure training of all new employees occurs before they have interactions with clients. When changes in risk i.e. geography, products or clientele we update training materials to ensure all members in the practice are aware of new risks presented.

4.5 – Relationship based risk assessment

Business *relationships* *Identify all your business relationships or high-risk clients (individually or as groupings) and assess as low or high*	**Rationale** *Explain why you assigned that particular rating*	**Describe enhanced measures** to ascertain ID for high-risk business relationships	**Describe mitigation measures, enhanced ongoing monitoring and process to keep client information up-to-date** for high-risk business relationships
Group A – LOW	Clients that conduct transactions face-to-face, or non-face-to-face with justifiable reason, in line with the client's profile i.e., occupation, source of 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. Politically Exposed Foreign Persons (PEFP) as a PEFP may be vulnerable to ML/TF or corruption due to their position, relationship or influence.	**Enhanced ID measures** Ensure ID is ascertained at time of application with a valid piece of photo identification issued by a federal or provincial government.	**Mitigation measures may include:** • Completion of the *Client risk assessment tool (see appendix)* documenting rationale for assessment. • Perform an internet search of the client to see if there is

Commented [MM15]: All factors assessed as high risk require enhanced measures to verify/ascertain ID. SAMPLE measures have been provided.

Commented [MM16]: 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.

	Clients for whom we are unable to obtain beneficial ownership information. This may indicate that the client is trying to hide the beneficial owner. A client that is an identified terrorist. A client with transactions sent to or received from North Korea (regardless of amount) Clients with a combination of potential high-risk triggers at on-boarding or as noted during ongoing monitoring that have been assessed and determined to be high risk. Potential high-risk triggers are listed in the risk assessment tool – See appendix.		any adverse media. **Keeping information up-to-date:** • Confirm/update client identification information with the client at every transaction and perform subsequent online searches. **Enhanced ongoing monitoring** • Review each transaction made by high risk clients at the time the transaction is conducted. ○ Maintain notes detailing the review of client transactions. ○ Compare the transaction to the purpose and nature of the business relationship. ○ Evaluate transaction against the client's profile. ○ Request additional information from client if transaction seems inconsistent with client profile. • Periodic review of client transactions

Commented [MM17]: 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 [MM18]: 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.

Section 5 – Timeframe for keeping records

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

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

We keep copies of suspicious transaction, large cash and terrorist property reports we have filed for at least five years following the date the report was made.

All other records are kept for at least five years following the date they were created.

Part D – Ongoing training program

All individuals within this practice who:

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

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

At SFG we use the modules provided to us through;

CAILBA

IFBC

Manulife Financial – Resource

INVESTIA Financial Services

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

Commented [MM19]: 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.

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 [MM20]: 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 [MM21]: 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, 2020*	

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:

Bedros SARKISSIAN

Date this program was adopted:

January 2011

Formatted: Font: Italic, Underline

Formatted: Font: Italic, Underline

Commented [MM22]: Record the date your practice adopted this program.

Formatted: Font: Italic, Underline

Formatted: Font: Italic, Underline

Part F – Program review

Policies

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

Commented [MM23]: This review can be completed by another employee or an outside consultant/auditor if feasible.

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: January 2017, 2015, 2013, 2011		
Completed by: Bedros SARKISSIAN		**Date: January 2017**
Results reviewed by: Denise SARKISSIAN		**Date: January 2017**
Compliance item reviewed	**Yes/No**	**Results of testing**
1) Appointment of a compliance officer		
Testing includes; a) Ensure a compliance officer has been appointed and approved by senior management	Yes	A compliance officer has been appointed as indicated in the program and the appointment has been approved by the principal as indicated in the compliance officer section of this program.
2) Written compliance policies and procedures are approved, effective and reflect current legislative obligations		
Testing includes: a) Confirm policies and procedures have been approved by the principal.	Yes	Policies and procedures have been approved by the principal as indicated in Part E - Approval and adoption of policies, procedures and training program.
b) Refer to the FINTRAC website to see if there are new legislative changes noted. If there are changes since the date of last review/revisions to this program, make updates as required to ensure program is up to date with FINTRAC guidelines.	Yes	Reviewed website, legislative changes effective June 2017 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 [L24]: The results of the program review need to be reviewed by the principal within 30 days of completing the review.

Commented [MM25]: 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.

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 and other factors and that assessments accurately reflect your 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 NA	Reviewed 10% of high risk clients, evidence of periodic review was noted. OR At this time there are no high risk clients identified in the practice
3)Program review has been completed at least every two years and results reviewed		
Testing includes: a)Confirm that a program review has been completed within the past two years	N/A YES	Implementation of this program replaces the existing program for this practice and as such as program review has not been completed in the past two years. Next program review will be scheduled for two years after implementation of this program or sooner if needed as noted in policies above. OR This program is the first program documented for the practice, a self review will be completed within two years. OR A self review was completed within the past two years, the next self review will be scheduled for two years from implementation of this program.
b) Confirm the review was signed off by the principal.	Yes	The results of this review were signed off as indicated above.

4)Ongoing compliance training – policies and procedures for the frequency and method of training are in place and effective		
Testing includes: a)Ensure frequency of training is detailed in the program.	Yes	The training program states that training will occur annually.
b) Ensure all employees that have exposure to client transactions have received training annually by viewing evidence of training completion.	Yes	Evidence of training maintained and reviewed to ensure that all required employees have received training.
Actions required **No actions required at this time.**		
Follow-up actions completed		

Commented [MM26]: Document any changes that need to be implemented as a result of the review.

Part G – Revision history

Commented [MM27]: Retain prior versions of your programs to demonstrate continuity. Record changes to this program here when/if you make changes.

Commented [L28]: Document the most recent revision date on the cover page of this program.

Date	Section changed	Reason for change

Appendix

Client risk assessment tool

Commented [MM29]: 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 (i.e., cash intensive businesses, off shore business, business in high risk countries, online gambling)
- Client's business structure or transactions seems unusually complex
- Non face-to-face client identification without justifiable reason

Geography:

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

Other suspicious transaction indicators:

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

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