(NAME OF MGA) ANTI-MONEY LAUNDERING AND

ANTI-TERRORISM FINANCING COMPLIANCE POLICIES AND PROCEDURES*

Effective Date:

Revised on:

Risk Assessment Date:

Self-Assessments/Reviews:

Compliance Officer:

Signature of Board Secretary or Most Senior Officer

Date:

*CAILBA Guidance on establishing an AML Compliance Regime is incorporated by reference in this document and forms part of our MGA's compliance regime.

Important Note: The CAILBA templates, including the Guidance Manual and Policies and Procedures, are created for MGAs in their traditional role.* If, however, you are a client-facing MGA, you must maintain certain records and take certain measures that would usually be confined to the role of an Advisor. We attempt to provide some guidance in this regard, but the MGA is ultimately accountable for ensuring that it complies with the rules that apply to its actual practices and that it amends this templated material accordingly.

* "Managing General Agent" means a legal entity authorized by an insurance company to recruit, train and manage individuals and corporate entities to solicit applications, facilitate transactions and provide advice and assistance regarding individual insurance and/or investment fund products offered by the insurance company.

OUR AML POLICIES

We will strictly adhere to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (Canada) ("Act") and its regulations. It is our policy to prohibit and to take all reasonable steps to prevent, detect and report possible money laundering, terrorist financing activities and suspicious transactions.

For the purposes of this Policy, money laundering is defined as engaging in acts designed to conceal or disguise the origins of funds derived from criminal activity in an effort to make those funds appear to derive from lawful activities.

Our employees are required to adhere to our policies and procedures in preventing the use of insurance products and services for money laundering and terrorist financing purposes. If there are any questions, please contact the Compliance Officer immediately.

No Cash Policy

Like most of the life insurance industry, we do not accept cash for payment. Consequently, we do not require a procedure for handling, recording or reporting large cash transactions. However, if there is any attempted large cash transaction, we will assess it to determine whether a STATR is required and will file any required reports.

Our Compliance Program

1. **Compliance Officer** – our Compliance Officer is identified on the front page of this manual. The Compliance Officer's job description and appointment are appended to this document and form part of our compliance program.

1. **Risk Assessment** – after a review of our business environment, including products, Advisors, distribution channels, geographical areas, internal risks, general client mix, technology, and insurers whose products we promote, we have identified areas that require more monitoring or extra controls. The Compliance Officer maintains copies of the risk assessment, which is completed at least every two years, and of certain client risk assessments for clients identified as high risk in our own book of business.

1. **Self–Assessment** – we perform a self-assessment of the effectiveness of our policies and procedures for maintaining records and making reports to FINTRAC every two years. The Compliance Officer maintains copies.

1. **Training** – we have developed a formal training plan for all employees. All new employees will be trained to identify and manage AML/ATF risks before they are entrusted with any work that requires this training. All employees will receive training that covers the topics required by FINTRAC as well as training targeted to the jobs they do. Refresher training will be conducted on at least an annual basis.

- **Policies and Procedures for Maintaining Records and Making Reports**

General AML/ATF – Minimum Compliance Procedures

1. When screening Advisors, we ask whether they have an AML regime in place. We will not contract with Advisors who have not implemented an AML compliance regime.
2. We provide Advisors with access to AML template material and information so that they can achieve compliance, including information about AML/ATF training, even if we do not deliver the training or pay for it.
3. We train staff handling screening and contracting, new business and in-force, to be sensitive to and identify riskier situations that need to be escalated. In addition, staff handling applications and in-force changes are asked to identify gaps in insurers' forms and in what Advisors submit, so that we can reach out to Advisors and attempt to complete our own records.
4. We review reports on sales and review a sampling of files at regular intervals to identify problem areas and to ensure that we are retaining the appropriate records.
5. We flag specific cases identified as higher risk in non-registered higher risk products and review them before processing.
6. We identify higher-risk Advisors and customers and monitor their cases more closely.

Once escalated to a Compliance Officer, a case should be reviewed closely. If necessary and prudent, the Advisor might be contacted to provide information or to contact the customer for information.

PROCEDURES FOR FILING REPORTS WITH FINTRAC

• STATR PROCEDURE:

A Suspicious Transaction is one that raises questions or gives rise to discomfort, apprehension or mistrust. Look for things that seem to be out of the normal and tryout your gut feelings in deciding when to escalate concerns.

- Escalate any concerns immediately to the Compliance Officer. While the Compliance Officer should not discuss whether a STATR report will be or has been filed, he or she may contact the insurer(s) involved to consult regarding the transaction.

- The Compliance Officer will immediately review **FINTRAC Guidance on Reporting Suspicious Transactions** to determine *whether* to report and *what* to report. If inquiries through the Advisor are required to reach the end customer, there is an enhanced likelihood that the customer would surmise that you we're making a report. This must be taken into account each time a Suspicious Transaction or Attempted Suspicious Transaction is identified, particularly if there are concerns about whether the Advisor is involved.
- Where a STATR has been filed, monitor policy level and customer level activity on any affected policies for which we have records and monitor the Advisor's book of business for some period of time.

We are required to retain a copy of the STATR. The instructions and codes for making electronic reports are housed ***(identify location in your offices).***

Time is of the Essence. STATR reports and any follow up requests by FINTRAC must be filed with FINTRAC as soon as practicable after the detection of a fact that constitutes "reasonable grounds".

1. **Terrorist Group or Listed Property Report Procedure:**

When an attempted or completed transaction is detected, the Compliance Officer should immediately review FINTRAC Guidance on Reporting Terrorist Property, which contains instructions on *what*, if any, reports must be made and to *which* entities.

    - Interview the person who claims to be in possession or control of terrorist property.
    - Consult the most current lists at https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/index.aspx?lang=eng&_ga=2.54237544.1991558184.1647821597-1192645042.1647821597
- Ensure that the property in question (most likely a premium payment, insurance policy, refund or payment of a benefit) ***is not processed.*** Under the Criminal Code, it may have to be frozen.
    - Flag the policy/associated policies/customer/Advisor on our administrative system and freeze activities or set up a manual process for monitoring.
    - Check with insurers as to their requirements for notification of this kind of report and inform them of the actions you have taken**.** The MGA and Advisor act on behalf of the insurer for this purpose, which technically holds the property and is responsible for making any required report. We are accountable for notifying the financial institution and cooperating with its requests for information. (In any instance where the Advisor is not acting on behalf of a financial institution, the Advisor is considered to be holding the property directly. This includes situations where the Advisor provides financial planning, tax or estate planning services, for example.).
- If a *non-staff* Advisor notifies the MGA that he or she may be in possession of such property, the Advisor is responsible for taking these steps, but the MGA's Compliance Officer may assist the Advisor.

Procedures for Maintaining Records

- **General Procedure for Ensuring Complete Records:**

As an MGA, we rely on the insurer to ask the right questions in its applications and forms and on the Advisor to supply the information required so that we can create a record. We operate on a best efforts basis.

These procedures apply to all whole life, universal life, non-registered segregated funds/other annuities and CI with return of premium, where premiums paid over the life of the policy would reach $10,000, or where the policy will remit an amount of $10,00 or more to a beneficiary over the duration of the policy:

    - Verify that the application or change form is in good order before passing it through to the insurer.
- Retain a copy of the record if the Advisor provides it.
- Send an email to the Advisor if anything is missing from the application. Ask for the information for your records and **retain a copy of the request** to demonstrate that you take reasonable measure.
- Create a record on the administrative system either by scanning the document with the record or inputting the required information.
- In the case of corporate clients, where the Advisor does not submit records that indicate appropriate signing authority and that establish the existence of the corporation, reach out to the Advisor or perform a corporate online search.
- Do not delay forwarding anything to the insurer unless the insurer has indicated that it will not accept the application or change without the information.
- The Compliance Officer may flag policy/associated policies/Advisor/customer for monitoring and reports or set up a manual process for monitoring.
- Always maintain a copy of any STATR you file with FINTRAC.

- **Procedure for Maintaining Information Records for Clients, Beneficial Ownership, Business Relationships and Beneficiaries:**

Reasonable measures: Although no longer required, if any of the following information is missing, it is prudent to email the advisor and ask them to provide the information to us. Keep a record of the request and response. If a client-facing MGA, these rules apply to the MGA directly.

ON JUNE 1, 2021, THE APPROVED METHODS FOR IDENTIFYING CLIENTS WERE AMENDED TO SIMPLIFY THE CLIENT IDENTIFICATION PROCESS. IF AN ADVISOR HAS ALREADY ASCERTAINED CLIENT IDENTITY UNDER THE OLD METHODS, THE ADVISOR IS NOT REQUIRED TO DO SO AGAIN. **SEE TABLES 1-4 FOR DESCRIPTIONS OF THE NEW METHODS AND ADDITIONAL INFORMATION.** ***SEE FINTRAC METHODS TO VERIFY THE IDENTITY OF PERSONS AND ENTITIES,*** **ANNEX 1 – 5 FOR DETAILS:**

HTTPS://FINTRAC-CANAFE.CANADA.CA/GUIDANCE-DIRECTIVES/CLIENT-CLIENTELE/GUIDE11/11-ENG#ANNEX1

For an individual – The Advisor or client-facing MGA must ascertain and record the client's name, address, date of birth and the nature of the client's principal business or occupation. In the case of a group life insurance policy or a group annuity, the client information record is about the applicant for the policy or annuity.

ALL DOCUMENTS USED TO IDENTIFY CLIENTS MUST BE AUTHENTIC, VALID AND CURRENT. INFORMATION FOUND THROUGH SOCIAL MEDIA IS NOT ACCEPTABLE.

While client identity for a large cash transaction record must be at the time of the transaction, client identity for a client information record must be done within 30 days of creating the record. This is true whether the transaction is conducted on the client's own behalf, or on behalf of a third party.

Note that some insurers will not allow all the methods of ascertaining identity and may place limitations on who may act as a mandatary. **See Table 1.**

Note that, regardless of the method used for ascertaining identity, the information (name, address, DOB) collected from the client must match the information you refer to. Otherwise you cannot rely on the information collected.

1. **Individual policies** – It is important to distinguish between owners and lives insured. The ID requirement pertains to owners, not lives insured.

- Owner's name,
- Owner's address with enough detail to ensure that the address can be located
- Owner's date of birth
- Owner's principal business or other occupation. Must be specific.
- Type of authentic, valid and current documents used to confirm identity. **See Table 1.**

Acceptable forms of ID – all must be valid and current and have a unique identifier number and have been issued by a provincial, territorial or federal government. **See Table 4.**

- **Ascertaining the Identity of a Child**

Information provided by a parent may be relied upon to record the identification of children 12 years old and younger. Children from 12-15 years old may be identified using one of the methods in the tables. In addition, the Advisor may rely on a source of information that contains the parent or guardian's name and address and a second source that contains the child's name and date of birth.

- **Non-face-to-face sales – See Tables 2 and 3.**

1. **Group policies:** "Client" for group sales means the applicant for the policy, not the certificate holder or life insured. The client is generally the corporation or other entity. See Corporate Ownership below.

1. **Corporate ownership:**

- Name and address of corporation,
- Names of the corporation's directors,
- The names and addresses of all individuals who directly or indirectly own or control 25% or more of the shares of the corporation, and
- Information on the ownership, control and structure of the corporation.
- If Paper record confirms existence – a copy must be retained.
- If Electronic record confirms existence – corporation's registration number and the type and source of the record.

If an Advisor does not produce the information:

- Consult Corporations Canada database at **http:/www.ic.gc.ca,** which will provide name and address of the corporation and he names of the directors**.**
- Maintain a copy of the search.

Acceptable documents for confirming a corporation's existence include:

- Certificate of corporate status
- A record that has to be filed annually under provincial securities legislation
- Corporation's annual report signed by an independent audit firm
- Letter or notice of assessment from a municipal, provincial, territorial or federal government.

Acceptable documents to confirm beneficial ownership of a corporation:

- Articles of incorporation
- Annual returns
- Shareholder agreements

- **Ownership by a Trust:**
- The names and addresses of all trustees and all known beneficiaries and settlors of the trust.
- Information on the ownership, control and structure of the trust.

- **For entities other than corporations or trusts:**
- The names and addresses of all individuals who directly or indirectly own or control 25% or more of the entity; and
- Information on the ownership, control and structure of the entity.

Acceptable documents for confirming the existence of entities other than corporations:

- Partnership agreement
- Articles of association or similar record.

Acceptable documents to confirm beneficial ownership of non-corporate entities

- Articles of constitution
- Partnership agreements
- Records of decisions
- Trust deed.

1. **Beneficiaries** – This ID requirement pertains to beneficiaries of policies.

- Beneficiary's name,
- Beneficiary's address with enough detail to ensure that the address can be located
- Beneficiary's date of birth
- Beneficiary's principal business or other occupation. Must be specific.
- Type of authentic, valid and current documents used to confirm identity. **See Table 1**.

Acceptable forms of ID – all must be valid and current and have a unique identifier number and have been issued by a provincial, territorial or federal government. **See Table 4.**

- **All Policies**

- **Where beneficial ownership cannot be determined or confirmed:**
- Record the name and identity of the most senior managing officer of the corporation, trust or other entity.
- **Escalate these cases to the Compliance Officer** because these must be treated as high risk and be monitored more frequently along with regular updates of client ID.

- Check to ensure that the **purpose for the insurance** is identified on applications, as this represents the nature of the Advisor's "**business relationship"** with the customer.

- **Other Records to be Maintained**

Not-for-Profit Organization:

- Record whether the customer is a charity registered with CRA or a non-registered entity that solicits charitable financial donations.
- Check CRA site https://www.cra-arc.gc.ca if information not provided.
- Escalate any non-registered charity cases to the Compliance Officer as these are automatically high risk.

THIRD PARTY DETERMINATION RECORD:

- **If Third Party is an Individual:**
- Third Party's Name
- Third Party's Address
- Third Party's DOB
- Third Party's principal business
- The nature of the relationship between the owner and the third party.
- Any suspicions of third party involvement identified by the Advisor or staff.

- **If Third Party is a corporation:**
- All of the above information (except DOB)
- Incorporation number
- Place of incorporation

Politically Exposed Person ("PEP") and Head of International Organization ("HIO") and family and close associates of either Record:

For all lump sum payments of $100,000 or more for an immediate or deferred annuity or life insurance policy, or for a beneficiary to whom a remittance of $100,000 or more over the duration of the policy:

The Advisor (or client-facing MGA) has 30 days from the date of the transaction to make the determination. The most senior manager must review all transactions involving PEPs and HIOs within that same 30-day period. Many insurers conduct daily foreign PEP searches on all clients, which is an additional control. See Guidance for description of who is included. **Treat all foreign PEPs as high risk.**

Following senior management review of the transaction, the record that must be created for all foreign PEPs and any domestic PEPs or HIOs or the high-risk family member or high-risk close associate of any of these must include:

- the office or position of the PEP or HIO,
- the organization or institution of the PEP or HIO,
- the source of funds, if known, for the transaction,
- the source of wealth, if known,
- the date the advisor made the determination,
- the name of the senior manager who reviewed the transaction,
- the date the transaction was reviewed, and
- the nature of the relationship between the client and the PEP or HIO, if applicable.

See Table 5 organizations that may trigger HIO requirements.

Beneficiary Reasonable Measures Record

The information record for the beneficiary must be created before the remittance of funds to the beneficiary. If you are unable to create the information record within the time period required due to facts or circumstances beyond your control, you need to document and keep evidence of this. The following information is to be included:

- Beneficiary's name
- Beneficiary's address with enough detail to ensure that the address can be located
- Beneficiary's date of birth
- Beneficiary's principal business or other occupation. Must be specific.
- Type of authentic, valid and current documents used to confirm identity. **See Table 1**.

Acceptable forms of ID – all must be valid and current and have a unique identifier number and have been issued by a provincial, territorial or federal government. **See Table 4.**

Ongoing Monitoring

Advisors are required to monitor their clients based on risk. Although we do not have business relationships and may not have sufficient information to identify level of risk, as part of our own due diligence, we review and flag Advisors and customers who could represent higher risk and establish processes, including:

- **Training staff to:**
- Pay particular attention to the sale of whole life, universal life and segregated funds, where we required customer ID and specific information for records.
- Identify higher-risk customers who may need more regular monitoring.
- Identify red flags that need to be escalated to the Compliance Officer.
- Escalate any sale of a high-risk product with a premium of (Identify your dollar tolerance) $_____ per year for management sign-off.

- **Monitoring Advisors who:**
- Are new to the business.
- Have just recently joined our MGA.

- Sell complicated, large premium high-risk policies.
- Specialize in sales to professional corporations.
- Have lower persistency and/or higher number of cases that lapse as a result of NSF cheques, cancellations, not-takens, withdrawals and termination of policies prior to the contract being issued.
- Have been flagged by management or the Compliance Officer based on:
- Years of experience
- Clientele/market and business relationships
- Geographic location or sales to newcomers to Canada or to customers with ties to foreign jurisdictions known to have weak AML-ATF controls or terrorist financing activities.

FOR CLIENT-FACING MGAS:

ENHANCED MEASURES FOR HIGH-RISK CLIENTS

We take enhanced measures to keep client identification information up to date and mitigate against the risks these clients may pose. The measures we take will depend on the risk the client poses, but may include:

- Establishing a premium amount of $_____, which would trigger a mandatory review by _____;
- obtaining additional information on the client (e.g., occupation, assets, information available through public databases, Internet, etc.)
- obtaining information on the source of funds or source of wealth of the client
- obtaining information on the reasons for intended or conducted transactions
- identifying patterns of transactions that need further examination
- increased monitoring of transactions
- increasing staff awareness of high-risk activities and transactions
- increasing internal controls of high-risk business relationships.

Archived Material

We maintain records of the changes made to our AML/ATF Compliance Program for review by FINTRAC.