COMPLIANCE PROGRAM FOR ANTI-MONEY LAUNDERING AND TERRORISM FINANCING

Advisor name/Corporation name

Compliance Officer:

Effective:
Revised on:

Table of Contents

RESOLUTIONS OF THE BOARD OF DIRECTORS OF
Name of Firm (The "Firm") EFFECTIVE DATE

WHEREAS the Firm must adopt a compliance program in order to comply with *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the "Act") applicable to its operations;

WHEREAS the Firm must ensure that persons that it hires and/or who act on its behalf, whether or not they have a sales license, comply with the same provisions;

WHEREAS in order to ensure compliance with the various applicable rules, the Firm wishes to adopt a compliance program and to appoint one or more persons to be responsible for the application of this program;

IT IS THEREFORE RESOLVED:

THAT the compliance program attached is hereby adopted by the Firm;

THAT [name(s) of person(s) in charge of compliance] is/are appointed as compliance officer(s) with regard to the Act;

THAT as compliance officer(s) [Name(s) of those in charge of compliance] is/are responsible for:

- Implementation and monitoring of the compliance program;
- Establishing and periodically revising the Firm's policies, procedures and risk assessment;
- Initial and continuing training of representatives, employees and persons acting for and on behalf of the Firm;
- Making necessary declarations and/or reports to the competent authorities;
- Immediately notifying the principal of the Firm of any known or presumed violation of the Firm's compliance program;

THAT the compliance officer(s) may obtain the assistance of another person to manage the Firm's compliance responsibilities provided that this person has the requisite experience and skills in respect of the compliance aspects that are entrusted to him or her, provided that the name of this person or these persons and his/her/their responsibilities are documented in the compliance program.

THAT [name of principal of the Firm] is authorized to sign documents and take any other measures required to give full effect to the resolutions herein.

The resolutions herein are adopted by the director(s) of the Firm as witnessed by his/her/their signature(s) below.

_____ _____
Compliance Officer Date

ACCEPTED BY THE COMPLIANCE OFFICER(S):

_____ _____
Compliance Officer (if more than one) Date

Section 1 - Reviews and amendments to the Compliance Program

This program was adopted on

Document revision history

Date	What changed?	Reason for the change

Section 2 - Self-review

To test effectiveness, a review of compliance policies and procedures, assessment of business' risks related to money laundering and terrorist financing including risk mitigation measures, and training is conducted every two years.

These reviews will help determine if my/our business has policies and procedures in place to comply with legislative and regulatory requirements, and whether those policies and procedures are being adhered to.

Date of review:

Name of person completing review:

Signature of principal/advisor: _____

Compliance items	Yes	No	Comments, Testing/Evidence of effectiveness
Appointment of a compliance officer			
1. I/We have appointed a Compliance Officer for the practice.			
Written compliance policies and procedures			
2. Within the past two years, I/we have reviewed the criteria and process for identifying and reporting suspicious transactions and terrorist property and have established policies and procedures in this regard.			
3. I/We are aware of and abide by the requirements under the legislation for record keeping.			
4. I/We have reviewed the requirements under the legislation for client identification and verification and collect all information required on product applications, or as required, for each particular line of business.			
5. I/We have reviewed the legislated requirements with respect to reporting large cash transactions and where applicable comply with the requirements.			
Money laundering and terrorist financing risk evaluation			
6. Within the past two years, I/we have reviewed and documented my/our business' exposure to risk and have taken special measures to lower high risks.			
Ongoing compliance training			
7. I/We have established standards for the frequency and method of training with documentation on file.			
8. Details of the specific training material (i.e.,			

what training was completed, who completed the training and when was it completed) are documented and on file? If not, provide details here.			

Actions required:

Details of follow-ups completed:

Section 3 - Risk assessment

MONEY LAUNDERING/TERRORISM FINANCING RISK ASSESSMENT
(Completed/revised on in accordance with FINTRAC's Guideline 4)

I/We must go through the exercise of analyzing clientele both within business relationships (as defined in legislation) and outside of them, products and services to evaluate my/our own risk based on my/our specific business model. A review of this analysis is conducted every two years and is considered with new clients outside my/our established clientele profile or changes to current client circumstance.

Clientele profile	**Yes**	**No**	**N/A**	**Risk Assessment L = Low M = Moderate H = High**	**Risk-mitigation steps**
Description of clientele					
Are any clients:					
-Politically exposed foreign persons?					
-Beneficial owners (non-individual clients: partnerships, associations, businesses, non-profit organization, trusts etc.)?					
-Interested third parties?					
Are you unable to obtain beneficial ownership information for clients if client is a corporation, trust or other entity?					
Knowledge of clientele:					
Does client identification take place other than face-to-face?					
Do any clients live outside Canada?					
Does the comparison between clients with similar profiles and high levels of assets or large transactions seem unreasonable?					
Do any clients seem to have excessive knowledge of local laws, regulations and rules?					
Do any clients use intermediate vehicles (such as corporations, trusts, foundations, partnerships) or other structures that do not seem usual for their business or seem very complex and unnecessary?					
Type of business:					
Are clients' businesses cash-intensive?					
Do client's businesses generate large amounts of cash for certain transactions that are not normally cash-intensive?					
Are any clients an intermediary or "gatekeeper" such as a professional that holds accounts for clients where the identity of the underlying client is not disclosed to you?					
Clientele profile	**Yes**	**No**	**N/A**	**Risk Assessment**	**Risk-mitigation steps**

				L = Low M = Moderate H = High	
Do any clients use unsupervised intermediaries within the relationship who are not subject to adequate anti-money laundering or anti-terrorist financing obligations?					
Do any clients deal offshore?					
Do any clients offer on-line gaming?					
Do any clients' business structure or nature of its business or relationship make it difficult to ascertain the identity of the true owners or controllers?					
Geographic					
Do any clients operate or undertake activities in any country identified by the Financial Action Task Force (FATF) as a high-risk jurisdiction in the fight against money laundering or terrorist financing or subject to a FATF statement? You can consult the High-risk and non-cooperative jurisdictions information on the FATF Web site at http://www.fatf-gafi.org (select the tabs labelled "Jurisdictions for which an FATF call for action applies" and "Other monitored jurisdictions").					
Do clients operate or undertake activities in any country identified as a financial secrecy haven or jurisdiction?					
Do clients operate or undertake activities in any country subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN)? In some circumstances, this will include sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized.					
Do clients operate or undertake activities in any country identified by credible sources as lacking appropriate money laundering or terrorist financing laws and regulations? *Credible sources are well-known bodies that generally are regarded as reputable. Including, but not limited to. International bodies such as the World Bank, the International Monetary fund, the Organization for Economic Co-operation as well as relevant national government bodies and non-governmental organizations.*					
Clientele profile	**Yes**	**No**	**N/A**	**Risk Assessment L = Low M = Moderate**	**Risk-mitigation steps**

				H = High	
Do clients operate or undertake activities in any country identified by credible sources as providing funding or support for terrorist activities					
Location of clientele					
Are any clients located in a known high crime rate area?					
Is there a significant and unexplained geographic distance between you and the location of clients?					
Are there frequent and unexplained movements of accounts or funds between institutions in various geographic locations or different institutions?					
Important internal factors					
Is Advisor/employee turn-over in your practice high?					
Products offered					
Product types					
Are the following products offered?					
-Temporary insurance (Term)					
-Whole Life					
-Universal Life					
-Non-registered individual annuities and investments					
-Registered individual annuities and investments					
-Annuities purchased with products of a life insurance policy					
-Group Insurance					
-Non-registered group plans allowing ad hoc contribution (not salary deducted or employer contribution)					
-Registered group plans					
Types of transaction and services					
Are the following types of transactions or services offered:					
-Premium/deposit coming from OR proceeds going outside of Canada					
-Significant premiums					
-Premium coming from/proceeds paid to third party					
-Early surrender of a policy					
-Non face-to-face transactions					
Products offered	**Yes**	**No**	**N/A**	**Risk Assessment L = Low M = Moderate H = High**	**Risk-mitigation steps**

-Transfer of ownership					
-Through trust or power of attorney					
Overall Risk Assessment					

Risk level assessment matrix

You may use the following matrix, as appropriate, when assessing the level of money laundering and terrorist financing risks of your products, services and clients.

Low	Moderate	High
•Stable, known client base	•Client base increasing due to branching, merger, or acquisition	•A large and growing client base in diverse geographic area
•No electronic transaction services or the Web site is informational or non-transactional	•You are beginning electronic transaction services and offer limited products and services.	•You offer a wide array of electronic transaction services (i.e., account transfers, or accounts opened via the Internet).
•There are few or no large currency transactions.	•There is a moderate volume of large currency or structured transactions.	•There is a significant volume of large currency or structured transactions.
•Identified a few high-risk clients and businesses	•Identified a moderate number of high-risk clients and businesses	•Identified a large number of high-risk clients and businesses
•Few international accounts or very low volume of currency activity in the accounts	•Moderate level of international accounts with unexplained currency activity	•Large number of international accounts with unexplained currency activity
•A limited number of fund transfers for clients, non clients, limited third-party transactions, and no foreign funds transfers	•A moderate number of fund transfers, a few international fund transfers from personal or business accounts with typically low-risk countries	•Frequent funds from personal or business accounts to or from high-risk jurisdictions, and financial secrecy havens or jurisdictions.
•Your business is located in an area known to have low crime rate.	•Your business is located in an area known to have moderate crime rate.	•Your business is located in an area known to have high crime rate.
•No transactions with high-risk geographic locations	•Minimal transactions with high-risk geographic locations	•Significant volume of transactions with high-risk geographic locations
•Low turnover of key anti-money laundering personnel and frontline personnel (i.e., client service representatives, tellers, or other personnel)	•Low turnover of key anti-money laundering personnel, but frontline personnel may have changed	•High turnover, especially in key anti-money laundering personnel positions

Section 4 - Policies & Procedures

1. Mandatory Reporting Requirements

1.1 Suspicious Transaction or Attempted Transaction Report (STATR)

a. Identifying suspicious transactions or attempted transactions
b. Indicators of suspicious transactions or attempted transactions - general
c. Indicators of suspicious transactions or attempted transactions – industry specific
d. Prohibited disclosure to clients
f. Copy of STATR

1.2. Large Cash Transaction Report (LCTR)

1.3. Terrorist Group or Listed Person Property Report

a. Definition of property regarding terrorist group and listed person
b. Reporting under the *Act*
c. Reporting under the *Criminal Code of Canada*
d. Reporting scenarios

1.4. Making Reports to FINTRAC

a. Electronic reporting
b. Report acknowledgement and correction requests
c. Paper reporting
d. Information to be contained in reports

2. Required Written Records and Client Identification Obligations

2.1 Client information record
2.2 Beneficial owners record
2.3 Ongoing monitoring of business relationship and related records
2.4 Not-for-profit organization record
2.5 Third party determination record
2.6 Politically exposed foreign person record
2.7 Record retention requirements

3. Adoption as Policies and Procedures

Appendix A - Descriptive Scenarios of Suspicious Life Insurance Transactions or Attempted Transactions
Appendix B – Methods of money laundering and terrorist activity financing
Appendix C – Undertakings of employees and advisors
Appendix D – Identification of clients
Appendix E – Process for reporting suspicious transactions and attempted suspicious transactions

1. Mandatory Reporting Requirements

The *Act* has three sections that deal with mandatory reporting requirements applicable to the life insurance industry; Suspicious transaction or attempted transaction reporting; Large cash transaction reporting; and Terrorist group and listed person property reporting. Life insurance agents and brokers are covered as a "reporting entity" (we) under the legislation.

1.1 Suspicious Transaction or Attempted Transaction Report (STATR)

We are required to submit a Suspicious Transaction or Attempted Transaction Report (STATR) if we have reasonable grounds to suspect that the transaction or attempted transaction is related to a money laundering or terrorist activity financing offence. The reporting of suspicious activity will require us, and/or our staff, to exercise judgment.

We have thirty (30) days, from the date on which we have reasonable grounds to suspect that the transaction or attempted transaction is related to a money laundering or terrorist activity financing offence to file our report. If suspicion occurs at the time of the transaction or attempted transaction, the 30-day reporting timeline begins at that time. If the suspicion occurs after the transaction or attempted transaction or after multiple transactions or attempted transactions, the 30-day reporting timeline begins at that later time. We are not permitted to tell the client that we have made a report.

FINTRAC will send us an acknowledgement message when our report has been received electronically. This will include the date and time our report was received and a FINTRAC-generated identification number. If our report contains incomplete information, FINTRAC may contact us by phone, or we can file an updated report using the identification number assigned to the original report.

This process must be completed within the 30-day time period, our obligation to report is not considered fulfilled unless the report is complete.

The *Act* states that no criminal or civil proceedings lie against a person or an entity for making a report in good faith. In other words, we cannot be sued for disclosing information to FINTRAC as long as the report has been made in good faith.

Failure to file STATRs carry a maximum $2 million fine and five years imprisonment.

There is no minimum dollar threshold for reporting a transaction.

See Appendix E - Process for reporting suspicious transactions and attempted suspicious transactions for copies of STATR reports.

We must take reasonable measures to ascertain the identity of the person with whom the transaction is being or has been conducted, unless we believe it would inform the person that the transaction and related information is being or would be reported.

The transaction has to occur in the course of our activities as a life insurance broker or agent.

a. Identifying suspicious transactions or attempted transactions
When looking at a transaction to determine if it is suspiciously related to a money laundering or terrorist activity financing offence, remember that *behavior* is suspicious, not people.

We must look at the overall picture and consider some of the following factors:

- Our knowledge of the client,
- Our knowledge of client's industry,
- In the context of the transaction; is this normal,
- Our understanding of money laundering and terrorist activity financing indicators.

When looking at the context of the transaction and what is normal, think of the following example: Would we consider it normal for a client to buy a whole life policy based on a needs analysis? The answer is probably yes. Would we consider it normal for a whole life policy buyer to be more interested in early redemption features than financial security needs? Probably not. As we can see the same insurance transaction can be normal in some circumstances but not in others.

What constitutes "reasonable grounds" must be decided in the context of what is reasonable under the circumstances, such as normal business practices and procedures within the client's industry, profession or environment.

b. Indicators of suspicious transactions or attempted transactions- general
The following is a sample of some 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 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.

c. Indicators of suspicious transactions or attempted transactions - industry specific
The following is a sample of some industry specific 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 proposes to purchase a life insurance product using a cheque drawn on an account other than his/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.
- Client cancels investment or insurance soon after purchase.
- Client shows more interest in the cancellation or surrender than in the long-term results of investments.
- Client makes payments in cash, uncommonly wrapped notes, with postal money orders or with similar means of payment.
- The duration of the life insurance contract is less than three years.
- The first (or single) premium is paid from a bank account outside the country.
- Client accepts very unfavorable conditions unrelated to his/her health or age.

For further examples, see Appendix A for *Descriptive Scenarios of Suspicious Life Insurance Transactions or Attempted Transactions.*

d. Prohibited disclosure to clients
No person or entity shall disclose that they have made a report or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun. Basically, we are prohibited by law to tell the client that we have filed a report under this *Act.* The clause '*with the intent to prejudice a criminal investigation*' may be a defense in case of accidental disclosure.

For more information on reporting suspicious transactions or attempted transactions, visit www.fintrac.gc.ca and refer to Guideline 2 – *Suspicious Transactions* and Guideline 3 – *Submitting Suspicious Transaction Reports to FINTRAC.*

e. Copy of STATR
Every person or entity who submits a STATR to FINTRAC, must keep a copy of the report. Copies will be maintained in Section 5 Declarations of suspicious transactions and suspicious attempted transactions.

See Appendix E - Process for reporting suspicious transactions and attempted suspicious transactions for copies of STATR reports.

1.2 Large Cash Transaction Report (LCTR)

Reporting entities which accept cash are required to send a Large Cash Transaction Report (LCTR) to FINTRAC within 15 days after the transaction in either of the following situations:

- Receipt of $10,000 or more in cash (Canadian dollars or its equivalent in any foreign currency) in the course of a single transaction; or

- Receipt of two or more cash amounts of less than $10,000 that total $10,000 or more from the same individual or on behalf of the same individual or entity.

  In this case, making a LCTR is required if the transactions were made within 24 consecutive hours of each other by or on behalf of the same individual or entity.

(Choose which of the two options is appropriate for your business)
We do not accept cash transactions. Therefore no measures or processes are necessary in our business. Further, in the event a large cash transaction is attempted, a STATR would be made. See Section 1.1 Suspicious Transaction or Attempted Suspicious Transaction Report (STATR).

OR
Since most if not all insurers do not accept cash transactions, declaration of such transactions should be limited.

For more information on reporting large cash transactions, visit www.fintrac.gc.ca and refer to Guideline 7 – *Submitting Large Cash Transaction Reports to FINTRAC.*

1.3 Terrorist Group or Listed Person Property Report

In cases where we are acting on behalf of a financial institution we are not holding any property. Rather the property is being held by the financial institution, and the requirements of this section will be performed by the financial institution.

In situations where we are holding property directly, the provisions of this section will apply.

a. Definition of property regarding terrorist group and listed person

FINTRAC defines 'property' as any type of real or personal property. This includes, but is not limited to, any deed or instrument giving title or right to property, or any deed or instrument giving a right to money or goods. For example, cash, bank accounts, insurance policies, money orders, real estate, securities (including mutual funds), and traveler's cheques. This can also include business assets such as a plant, property, and equipment.

According to FINTRAC, a terrorist or a terrorist group can include an individual, a group, a trust, a partnership or a fund, an unincorporated association or an organization that facilitates or carries out any terrorist activity as one of their purposes or activities and will also include anyone on the list published in Regulations issued under the *Criminal Code*. Under the *Criminal Code,* 'terrorist group' has a similar meaning to FINTRAC and includes a listed entity.

The *Criminal Code* defines 'listed entity' as including a person, group, trust, partnership or fund or an unincorporated association or organization that has been placed on a list by the Governor in Council. This is done on the recommendation of the Minister, where the Governor in Council is satisfied that there are reasonable grounds to believe that the

entity has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or the entity is knowingly acting on behalf of, at the direction of or in association with a listed entity. The term 'listed person' is defined under the *Regulations Implementing the United Nations Resolution on the Suppression of Terrorism* to be a person whose name appears on the list that the Committee of the Security Council of the United Nations established and has a similar meaning to the definition in the *Criminal Code.*

b. Reporting under the *Act*
As a "reporting entity", we have a legal obligation to send a terrorist property report to FINTRAC if we have property in our possession or control that we **know** is owned or controlled by or on behalf of a terrorist group or listed person. This includes information about any transaction or attempted transaction relating to that property. All Terrorist Group and Listed Person Property Reports must be sent by paper as they cannot be sent electronically.

For more information on reporting a terrorist group and listed person property, visit www.fintrac.gc.ca and refer to Guidelines 5 – *Submitting Terrorist Property Reports to FINTRAC.*

c. Reporting under the *Criminal Code of Canada*
In addition to making a Terrorist Group or Listed Person Property Report to FINTRAC under the *Act*, the *Criminal Code* also has reporting requirements for terrorist property. These *Criminal Code* requirements apply to every person in Canada and any Canadian outside of Canada. It does not matter whether we are a reporting entity under the *Act* or not and we do not have to be involved in any life insurance transactions before we are subject to the *Criminal Code* requirements.

The *Criminal Code* requires us to disclose to the RCMP and CSIS the existence of property in our possession or control that we **know** is owned or controlled by or on behalf of a terrorist group or listed person. This includes information about any transaction or attempted transaction relating to that property. Information is to be provided to the RCMP and CSIS, **immediately,** at:

- RCMP - Financial Intelligence Task Force unclassified fax: (613) 993-9474.
- CSIS Financing Unit, unclassified fax: (613) 231-0266.

If we have property in our possession or control that we ***know*** is owned or controlled by or on behalf of a terrorist group or listed person, including information about any transaction or attempted transaction relating to that property, we may not complete or be involved in the transaction or attempted transaction. It is an offence under the *Criminal Code* to deal with any property if we know that it is owned or controlled by or on behalf of a terrorist group or listed person. It is also an offence to be involved in any transaction in respect of such property. In such circumstances, we are to remove ourselves from any involvement.

The *Criminal Code* has a 10-year maximum jail term for failure to report terrorist property to the RCMP and CSIS.

d. Reporting scenarios
There are four scenarios that can arise and our course of action depends on which set of circumstances is present. In all cases, if we have been involved in a life insurance transaction we may have a reporting obligation to FINTRAC and under the *Criminal Code.* If we have not been involved in a life insurance transaction, then our only potential reporting obligation will be under the *Criminal Code.*

Scenario 1 - If we ***do not know*** that the property in our possession or control is terrorist property and we ***do not suspect*** that it is, there is no obligation to report to FINTRAC under the *Act* or under the *Criminal Code.*

Scenario 2 - If we ***do not know*** that the property in our possession or control is terrorist property but ***we suspect*** that it is, there is no obligation to file a Terrorist Group or Listed Person Property Report to FINTRAC under the *Act* or disclose it to the RCMP and CSIS under the *Criminal Code.* In this circumstance we will have to file *a* ***Suspicious Transaction or Attempted Transaction Report*** regarding such property**.**

Scenario 3 - If we have property in our possession or control that we ***know*** *is* owned or controlled by or on behalf of a terrorist group or listed person, including information about any transaction or proposed transaction relating to that property, AND we have been involved in a life insurance transaction, we must file a Terrorist Group or Listed Person Property Report to FINTRAC and disclose it to the RCMP and CSIS under the *Criminal Code.*

Scenario 4 - If we have property in our possession or control that we ***know*** *is* owned or controlled by or on behalf of a terrorist group or listed person, including information about any transaction or proposed transaction relating to that property, BUT we have not been involved in a life insurance transaction, we must disclose it to the RCMP and CSIS under the *Criminal Code.*

1.4 Making Reports to FINTRAC

a. Electronic reporting
We must submit all reports electronically, if we have the technical capabilities to do so, except for the Terrorist Group or Listed Person Property Reports which can only be paper filed at this time.

Electronic reporting must be done by logging on to FINTRAC's secure web site (F2R). All reporting entities must register for and utilize F2R if they have the technical capability. Generally ‘technical capability’ means a computer and Internet access. This can be done via FINTRAC’s website at www.fintrac.gc.ca.

b. Report acknowledgement and correction requests
FINTRAC will send us an acknowledgement message when our report has been received electronically. This will include the date and time our report was received and a FINTRAC-generated identification number. Keep this information for our records.

If our report contains incomplete information, FINTRAC may notify us. The notification will indicate the date and time our report was received, a FINTRAC-generated identification number, along with information on what must be completed.

Any additional or incomplete information must be sent to FINTRAC within 30 days of the time the suspicion was first detected. Our obligation to report will not be fulfilled until we send the **completed** report to FINTRAC. In light of this 30-day requirement, we will make reports as quickly as possible to leave us enough time to respond to any correction requests.

c. Paper reporting
In the event we are unable to report electronically or we have to file a Terrorist Group and Listed Person Property Report, we must submit paper reports to FINTRAC. The following forms can be accessed and printed from FINTRAC's website or call 1-866-346-8722 for a copy to be faxed or mailed to us.

- Suspicious Transaction or Attempted Transaction Report (FINTRAC may refer to this report as a Suspicious Transaction Report)
- Large Cash Transaction Report
- Terrorist Group or Listed Person Property Report (FINTRAC may refer to this report as a Terrorist Property Report)

To ensure that the information provided is legible and to facilitate data entry, FINTRAC prefers the free-text areas of the paper report (such as, fields 1 and 2 of Part B) are keyed. If reports must be completed by hand, the use of black ink, and CAPITAL LETTERS is recommended.

There are two ways to send a paper report to FINTRAC:

- Fax: 1-866-226-2346; or
- Registered mail to the following address:
  Financial Transactions and Reports Analysis Centre of Canada,
  Section A,
  234 Laurier Avenue West, 24th Floor, Ottawa, ON K1P 1H7

FINTRAC will not send us any acknowledgement when a paper report has been received.

d. Information to be contained in reports
The information to be contained in reports depends on the type of report being filed. There are several parts that must be completed on both the *Suspicious Transaction or Attempted Transaction Report* form and the *Large Cash Transaction Report* form, but some parts are only to be completed if applicable. Any fields marked with an asterisk (*) must be completed. All other fields require us to make a reasonable effort to get the information. The information that is required to be provided includes:

- Information about the reporting entity (us).
- Information about the transaction or attempted transaction and its disposition.
- Information about the individual conducting a transaction or attempting to conduct a transaction and/or the individual on whose behalf the transaction is being conducted or attempted to be conducted.
- Information explaining our reasons for suspicion and if we have taken action.

One of the requirements for reporting large cash transactions is that multiple transactions under $10,000 each within a 24-hour period that exceed $10,000 in aggregate must be reported if we are aware that the transactions were conducted by, or on behalf of, the same person or entity. Certain information for some mandatory fields on the LCTR may not be available because the individual transactions were under $10,000. In this case, "reasonable efforts" can now apply to those mandatory fields on the LCTR. This means that if information was not obtained at the time of the transaction because it was under $10,000 and it is not available from our records we can leave the applicable LCTR field blank.

With Suspicious Transaction or Attempted Transaction Reports, we should use field “G1” to record the details of the transaction or attempted transaction and why we felt it was suspicious.

2. Required Written Records and Client Identification Obligations

Reporting entities are required to keep large cash transaction records if cash is accepted, and client information records. Other records that we are required to keep include records related to beneficial ownership, not-for-profit organizations, third party determinations, and politically exposed foreign persons.

2.1Client information record

If clients pay $10,000 or more for an annuity or a life insurance policy, over the duration of the annuity or policy, we keep a client information record regardless of how the client paid for the annuity or policy, whether or not it was in cash.

For an individual - We 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.

Client identity must be verified. Client identity for a client information record, must be done within thirty (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. However, if we have reasonable grounds and supporting evidence to believe that another life insurance company, broker or agent has confirmed the individual's identity, we do not have to confirm his/her identity again unless we have doubts about the information collected.

Unless otherwise specified, only original documents that are valid and have not expired may be referred to for the purpose of ascertaining identity. The identity is to be ascertained by reference to the individual's:

- Birth certificate;
- Driver's license;
- Provincial health insurance card (where allowed);
- Passport; or
- Any similar record.

If we are required to ascertain the identity of an individual purchasing an annuity or life insurance policy, the client information record has to contain the individual’s date of birth

along with the type of identification document used to confirm the individual's identity, its reference number and its place of issue.

See Third party determination record (below).

For a corporation - We must ascertain the existence, name and address of the corporation, and the names of its directors. This can be done by reference to:

- Certificate of corporate status;
- A record that it is required to file annually under the applicable provincial securities legislation; or
- Any other record that ascertains its existence as a corporation.

Such a record may be in paper form or in an electronic version that is obtained from a source accessible to the public. If paper, the individual or entity ascertaining the corporate identity must retain the record or a copy of it. If electronic, a record must be kept setting out the corporation's registration number, the type of record referred to and the source of the electronic version of the record. If the corporation is a securities dealer, we do not have to ascertain the names of the corporation's directors.

See Section 2.2, Beneficial owners record, Section 2.4, Not-for-profit organization record, and Section 2.5, Third party determination record (below).

For a non-corporate entity - We must confirm its existence by reference to a partnership agreement, articles of association, or any other similar record that confirms the entity's existence. We must keep a record of the type and source of records consulted or a paper copy of that record.

See Section 2.2, Beneficial owners record, Section 2.4, Not-for-profit organization record, and Section 2.5, Third party determination record (below).

In a **non-face-to-face situation -** If we have to identify an individual who is not physically present refer to *Verifying the identification of clients not physically present* section Appendix D - Identification of clients, for procedures and forms used and required by insurer we represent.

2.2 Beneficial owners record

If the client is a corporation, we must, at the time the existence of the corporation is confirmed, obtain,

- The name and, where required by a financial institution, occupation, of all directors of the corporation and, take reasonable measures to confirm and, keep a record of such.
- The name, address and, where required by a financial institution, occupation, of all persons who own or control, directly or indirectly, 25 per cent or more of the shares of the corporation and,
- Information on the ownership, control, and structure of the corporation.

We must search through as many levels of information as necessary in order to determine beneficial ownership. If there is no individual who owns or controls 25% or more of an entity we still keep a record of the measures we took and the information we

obtained in order to reach that conclusion. A beneficial owner cannot be another corporation or another entity.

If the client is a trust, we must obtain and keep a record of the names and addresses of all trustees and all known beneficiaries and settlors of the trust; and information on the ownership, control and structure of the trust.

If the client is an entity but not a corporation or a trust, we must, at the time the existence of the non-corporation entity is confirmed, obtain and keep a record of the name, address and, where required by a financial institution, occupation, of all persons who own or control, directly or indirectly, 25 per cent or more of the non-corporation entity; and information on the ownership, control, and structure of the entity.

If any of the information in this subsection cannot be obtained or its accuracy cannot be confirmed, we have to:

- Obtain the name of the most senior managing officer of the corporation, trust or other entity;
- Take reasonable measures to ascertain the identity of the most senior managing officer of the corporation, trust or other entity; and
- Treat that corporation, trust or other entity as high risk in our risk assessment document of our compliance regime.

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

In the context of this section, a senior managing officer of an entity may include but is not limited to its director, chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, as well as any individual who performs any of those functions. It also includes any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer. In the case of a sole proprietor or a partnership, the senior managing officer can be the owner or the partner.

We also have to keep a record of this information.

Keeping beneficial ownership information up to date is part of our ongoing monitoring obligations. The frequency with which we review beneficial ownership information and keep it up to date will vary depending on our risk assessment of our client. For high-risk clients, we will update beneficial ownership information more frequently and perform more frequent monitoring. See risk mitigation steps included in Section 3 - Risk assessment.

2.3 Ongoing Monitoring of Business Relationship and Related Records

Business relationship
A business relationship is a relationship that we establish with a client to conduct financial transactions or provide services related to those transactions. This term as it applies to anti money laundering and anti terrorist financing has been defined in order to clarify when a client is subject to enhanced monitoring.

We enter into a business relationship when we conduct two or more transactions in which we have to:

- Ascertain the identity of the individual or entity; or
- Confirm the existence of a corporation or other entity.

If we have a client who conducts two or more suspicious transactions, even if we are unable to ascertain the identity of the client, we have still entered into a business relationship with that client. This is because suspicious transactions require us to take reasonable measures to identify the client, and so two or more of these transactions will trigger a business relationship. We must treat this business relationship as high-risk, and undertake more frequent ongoing monitoring and updating of client identification information, as well as any other appropriate enhanced measures.

Once the business relationship is established, we must also:

- Conduct ongoing monitoring of our business relationship with the client; and
- Keep a record of the measures taken to monitor the business relationship and the information obtained as a result.

Ongoing monitoring

Ongoing monitoring means monitoring the business relationship with a client on a periodic basis. Using the risk assessment of the client with whom we have a business relationship we will determine how frequently we will monitor that business relationship. High-risk clients will be monitored more frequently and with more scrutiny than low-risk clients.

The risk assessment requires us to consider each one of the clients when assessing their risk for money-laundering and terrorist activities financing. However, an individual written assessment is not required for each client, so long as we can demonstrate that we put our client in the correct risk category, according to our policies and procedures, and risk assessment. We have to perform ongoing monitoring of each business relationship to:

- Detect suspicious transactions that have to be reported;
- Keep client identification, beneficial ownership information, and the purpose and intended nature of the business relationship up to date;
- Reassess the level of risk associated with the client's transactions and
- Determine whether the transactions or activities are consistent with the information previously obtained about the client, including the risk assessment of the client.

Business relationship record

When we enter into a business relationship with a client, we have to keep a record of the purpose and intended nature of the business relationship. We also have to review this information on a periodic basis and keep it up to date. This is done to ensure that we continue to understand clients' activities over time so that any changes can be measured to detect high risk, thus increasing the frequency of ongoing monitoring, updating of client identification information, and any other appropriate enhanced measures.

The frequency with which business relationship information is to be kept up to date will vary depending on our risk assessment of the client. We will monitor business relationships we consider high risk more frequently.

To obtain information on the purpose and intended nature of a business relationship, we can use the information we currently have about the client in our business records. If it's a new business relationship, one way of obtaining this information is to ask our client.

2.4 Not-for-profit organization record

If we have to confirm the existence of an entity that is a not-for-profit organization, we also have to do the following:

- Determine whether or not that entity is a registered charity for income tax purposes and keep a record to that effect. To make this determination, we can ask the client or consult the charities listing on the Canada Revenue Agency website (http://www.cra-arc.gc.ca).
- If that entity is not a registered charity, determine whether or not it solicits charitable financial donations from the public and keep a record to that effect. To make this determination, we can ask the client.

2.5 Third party determination record

A third party is an individual or entity other than the individual who conducts the transaction. When determining whether a "third party" is involved, it is not 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 us is acting on someone else's instructions. If so, that someone else is the third party.

If we are required to obtain a third party disclosure statement, that statement must include:

- The third party's name, address and principal business or occupation;
- Where the third party is an individual, date of birth;
- Where the third party is a corporation, the incorporation number and place of incorporation;
- Where the person or entity is acting on behalf of a third party, the nature of the relationship between the third party and the individual who signs the statement.
- Where the person or entity is not able to determine if the individual is acting on behalf of a third party but there are reasonable grounds to suspect that the individual is acting on behalf of a third party, a signed statement from the individual stating that they are not acting on behalf of a third party.

2.6 Politically exposed foreign person record

We must take reasonable measures to determine if a person who makes a lump-sum payment of $100,000 or more in respect of an immediate or deferred annuity or life insurance policy on their own behalf or on behalf of a third party is a politically exposed foreign person (PEFP).

A 'politically exposed foreign person' is a person who holds or has held one of the following offices or positions in or on behalf of a foreign state:

- head of state or head of government;
- member of the executive council of government or member of a legislature;
- deputy minister or equivalent rank;
- ambassador or attaché or counselor of an ambassador;

- military officer with a rank of general or above;
- president of a state-owned company or a state-owned bank;
- head of a government agency;
- judge;
- leader or president of a political party represented in a legislature; or
- holder of any prescribed office or position. It includes any prescribed family member of such a person.

For the purpose of the definition of a PEFP, the prescribed family members of a politically exposed foreign person are;

- the person's spouse or common-law partner;
- a child of the person;
- the person's mother or father;
- the mother or father of the person's spouse or common-law partner; and
- a child of the person's mother or father.

Being a Canadian citizen **DOES NOT** discount a client from being a politically exposed foreign person. A Canadian citizen who holds or has held a prescribed position on behalf of a foreign country would be considered a PEFP. For example, a Canadian citizen that works for a foreign embassy outside of Canada as an attaché of an ambassador would be considered a PEFP.

Conversely, a foreign national holding a similar political, judicial or military position on behalf of Canada, would not be considered a PEFP.

Once we have determined a client is a PEPF, we must take reasonable measures to establish the source of the funds that have been used for the transaction in question, the transaction must be reviewed by a member of senior management, and the review must be completed within 14 days after the day on which the transaction occurred.

Once we have determined that an individual is a politically exposed foreign person, we will not have to do it again. However, if we initially determined that an individual was not a politically exposed foreign person, we must still take reasonable measures to determine whether we are dealing with a politically exposed foreign person for every subsequent account opening or for prescribed electronic funds transfers, since the client's status may have changed.

If assistance is require, contact Market Conduct at MKTCONDUCT@canadalife.com

Forms and additional procedures
See Appendix D – Identification of Client for the procedures and sample forms used and required by insurers with which we're contracted for the identification of clients.

2.7 Record retention requirements
The requirements for record retention states that the records may be kept in machine-readable form provided a paper copy can be readily produced from it; or in electronic form, again provided a paper copy can be produced from it and there is an electronic signature of the individual who must sign the record.

These records are to be kept for a period of five (5) years from the day they were created and in some cases from the date of the last transaction conducted.

The records we are required to keep shall be retained in such a way that they can be provided to FINTRAC (or a FINTRAC authorized person) within 30 days after a request is made to examine them.

3. Adoption as Policies and Procedures

[Name of corporation's principal/advisor] declare having read and accepted this document as policies and procedures for [Name of corporation/advisor].

SIGNED AT _____ ON _____ 20__.

_____

[Name of corporation principal/advisor]

Appendix A
Descriptive scenarios of suspicious life insurance transactions or attempted transactions

NO PICTURE ID - Fact: A potential client meets with you to purchase a life insurance policy or an annuity. You ask the person for a Driver's Licence or Passport. The potential client shows a "passport" with no picture and when questioned by you says that it is a military passport and that military passports do not have pictures. When asked for another form of ID, the person, unable to produce another ID, becomes irate and questions whether the insurance company wants her business or not.

CHANGE IN PAYMENT BEHAVIOUR - Fact: You notice that for the third Friday in a row a small business owner gave you a payment of exactly $9,500 in money orders to add to his individual variable insurance contract.

HIGH RISK BUSINESS - Fact: A jeweler/precious metal dealer applies for a corporate owner life insurance policy. In accordance with due diligence procedures for owners in high risk businesses, the dealer provides valid articles of incorporation and documents that verify its identity is accurate and complete. You notice that on the first of every month, the dealer calls in requesting a loan, which is immediately paid back with cash equivalents.

DISREGARD FOR MONETARY LOSS - Fact: An annuity owner calls you to request a surrender of an annuity, which was held for less than one year. When you apprise the owner of the surrender charges and potential losses, the owner indicates that the fees and losses do not matter and to please make the surrender immediately and wire the money to an account located in Europe.

FOREIGN CLIENTS AND OVERSEAS MARKETS – Fact: On taking care of business, you heard that two of your clients are currently residing in North Korea. You also know that the address of record of both clients is in your province. Both contracts have been in force for approximately 10 years.

Upon further investigation, you learn that one client is currently in North Korea but the owner of the policy resides in your province. The other client, who is the owner and insured of her policy, is also currently living in North Korea. Both policies were issued in Canada and premiums are being paid via electronic bank drafts with funds from Canadian credit unions.

KNOW YOUR CLIENT - Fact: You have written an application for life insurance and the client provides payment to you in the form of eighteen money orders totaling $9,088, ranging from $88.00 to $1,000 in amount.

The prospective insured is a 25-year old male who does not have a chequing account. The application shows Columbia as country of birth, and a current address in another province. The application also indicates that the proposed insured is the business owner of a Columbian restaurant in your own community.

SUSPICIOUS TRANSACTION MONITORING - Fact: You receive what appears to be a $15,000 bank draft from Tulips Bank in The Netherlands for payment of insurance premiums. The insured's

name and policy number are written on the cheque, which appears to be in U.S. dollars. The name of a not-for-profit organization is printed toward the bottom of the cheque.

CRIME CONNECTION AWARENESS - Fact: You become aware through the media that a long-standing client was involved in organized crime activities in a foreign country. The insurance policies were of 29 years duration. One provided for a payment of close to $1 million in case of death. The other was a Universal Life product with value of over half this amount.

USE OF COOLING OFF PERIOD - Fact: You discover an instance where the single life insurance premium has been paid in Canadian currency and the request for a refund under the 10-day free look is to be paid in another currency.

CORRUPTED INFORMATION - Fact: A client is being referred to you by an insurance company employee with the information that payment for the policy will be made by two separate wire transfers from overseas accounts because the funds used for payment are the proceeds of overseas investments. The employee indicates that the client is well known to the insurer, there are no reasons for concern, and strict compliance need not be adhered to in this case.

MULTIPLE POLICIES - Fact: In taking care of business, you find out that a client has purchased life insurance policies from a number of insurance companies. In every case, the insurer was requested to provide life coverage with an indemnity value identical to the premium. There were also indications that in the event that the policies were to be cancelled, the return premiums were to be paid into a bank account in a different jurisdiction to the insured.

INSURANCE EXCEEDING NEEDS - Fact: After you have done a thorough life insurance needs analysis, the client insists on buying twice the needed amount for greater financial security. In discussing coverage and payment, you notice that he shows more interest in the cancellation or surrender than in long-term coverage.

REPEATED BENEFICIARY CHANGES - Fact: You are contacted by a potential client who wants to buy life insurance with duration of less than three years. Three months after the establishment of the policy, the beneficiary is altered. The policyholder calls you again two months before the expiry of the insurance for another beneficiary change. The insured remained the same.

KNOWLEDGEABLE CLIENTS - Fact: In purchasing an annuity, the client appears to be very conversant with money laundering or terrorist activity financing issues and she is quick to volunteer that the funds are "clean". She goes on to say that annuity products are well suited to "layering".

SPECIAL FAVOURS OFFERING - Fact: While providing life insurance advice, the client offers you money, gratuities or unusual favors for the provision of services that may seem unusual or suspicious such as sending correspondence to an address other than his home address, insisting that the transaction be done quickly or establishing identity using something other than his personal identification documents.

Appendix B
Methods of money laundering and terrorist activity financing

Methods of money laundering
There are many known methods to launder money and more are being devised every day. The methods are becoming more sophisticated and complicated as technology advances. Some of the most common methods are:

- ***Nominees -*** use of family members, friends, or associates who are trusted within the community and who will not attract attention. This facilitates the concealment of the source and ownership of the funds involved.
- ***Structuring (smurfing) -*** inconspicuous individuals deposit cash, buy bank drafts, or money orders at various institutions, usually for amounts less than the thresholds for reporting. The drafts or money orders are usually made payable to other parties and, along with cash, are typically deposited to a central account.
- ***Bulk cash asset purchases -*** individuals buy big-ticket items like cars, boats, and real estate for cash. Often these will be registered in other names to distance the launderer. The assets can then be sold and converted back to 'clean' cash.
- ***Currency smuggling -*** funds are moved across borders to other countries to disguise the true source and ownership of the funds. They are typically taken to countries where there are few, if any, laws to record the ownership of funds entering the financial system. These countries tend to also be those with very strict bank secrecy laws. Methods for smuggling include mail, courier, and body packing.
- ***Exchange transactions -*** proceeds of crime are used to buy foreign currency that can then be transferred to offshore bank accounts or converted back to functional currency at another institution.
- ***Casino gambling -*** individuals bring cash into a casino and buy casino chips/tokens. After gaming and placing a few small bets, they redeem the remainder of the chips/tokens and request a casino cheque (often made payable to a third party).
- ***Black market peso exchange -*** this is a method primarily affecting the United States although Canada is not immune to it. There is an underground network of currency brokers who buy the US and Canadian dollars from the criminal and give them pesos. The brokers then sell these US and Canadian dollars to foreign companies for pesos who use the funds to purchase goods in the US and Canada for sale back home.

Methods of terrorist activity 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.

- **Financial support -** Terrorism could be sponsored by a country or government, although this is believed to have declined in recent years. State support may be replaced by support from other sources, such as individuals with sufficient financial means. This could include, for example, donations to certain organizations that are known to have links to terrorists or terrorist groups.

- **Revenue-generating activities -** The revenue-generating activities of terrorist groups may include criminal acts, and therefore may appear similar to other criminal organizations. Kidnapping and extortion can serve a dual purpose of providing needed financial resources while furthering the main terrorist objective of intimidating the target population. In addition, 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. Only a few non-profit organizations or supposedly charitable organizations have been implicated in terrorist financing networks in the past worldwide. In these cases, the organizations may in fact have carried out some of the charitable or relief work. Members or donors may have had no idea that a portion of funds raised by the charity was being diverted to terrorist activities. This type of "legitimately earned" financing might also include donations by terrorist group members of a portion of their personal earnings.

  The methods used by terrorist groups to generate funds from illegal sources are often very similar to those used by "traditional" criminal organizations. Like criminal organizations, they have to find ways to launder these illicit funds to be able to use them without drawing the attention of the authorities. For this reason, transactions related to terrorist financing may look a lot like those related to money laundering.

  Therefore, a robust comprehensive anti-money laundering regime is key to providing the information necessary to identify and track terrorists' financial activities.

Appendix C
Undertakings of employees and advisors of (corporation/advisor)

All employees and advisors are required to read the Policies and Procedures so that they have enough information to process and complete a transaction properly as well as to ascertain the identity of clients, keep records as required and know when an enhanced level of caution is required in dealing with transactions.

I have read (corporation/advisor's name) Policies and Procedures for the fight against money-laundering and terrorism financing and I am familiar with these Policies and Procedures and agree to comply with them.

SIGNED AT _____ ON _____.

_____
Name:

_____
Title:

_____
Signature:

Appendix D
Identification of clients

Procedures are contained in the Client Information record section. Additional procedures and forms are used and required by insurers for the identification of clients.

Verifying the identification of clients not physically present

Normally, verifying the identification of a client can be accomplished during face-to-face meetings, by viewing the original copy of his/her driver's licence, passport or other acceptable identification, and providing the document number and issue/expiry date on the application form.

However, we are also obligated to certify the identity of the applicant/owner on the rare occasions when the individual is not physically present during the application process. In these cases, the following processes needs to be followed:

For individual universal life insurance polices
In cases where the applicant/owner is not seen the forms mentioned below are required for the application process and can be downloaded from the advisor portal under Forms & procedures, life insurance form administration.

- The Certification of personal identity – 17-8296 must be provided to the applicant/owner. He/she is required to have an acceptable individual (as defined on the form) validate their identification.

- The Confirmation of account –17-8333 must be completed by someone at the applicant's/owner's bank or trust company. It verifies the applicant/owner has a non-registered account with the institution.

Completed forms must be submitted to the business area before the policy can be issued.

For investment products
Situations where the client is not seen will be treated on an exception basis as the risks of money laundering and terrorist financing are greater within the investment industry. Contact IRIS Compliance for further information, prior to doing business with a client who is not physically present.

Politically exposed foreign persons (PEFP) and beneficial owners

LIFE INSURANCE	Beneficial owner	Politically exposed foreign person (PEFP)
Millennium universal life insurance *Simply Preferred* term life insurance Participating life insurance (*Wealth Achiever, Estate Achiever)*	When corporation or other entity is applying for or converting an existing policy to a universal life policy, regardless of the amount of premium: • Complete and submit the Questionnaire for Applicants / Owners which are Entities (form 17-8295) with the application • Located on Canada Life™ *RepNet* under Forms & procedures > Compliance.	A *Politically exposed foreign person determination* (form 17-8294) is required on <u>any</u> policy for each person who is the applicant, policyholder or payor: • If the initial scheduled payment is $100,000 or more. It is not required for subsequent scheduled payments. • For any <u>un</u>scheduled payment of $100,000 or more Complete *Politically exposed foreign person determination (PEFP)* (form 17-8294) located on Canada Life™ *RepNet* under Forms & procedures > Compliance.
INVESTMENTS	**Beneficial owner**	**PEFP**
Canada Life Generations™ Guaranteed products Payout annuities	For all **non**-individual policies (e.g. corporate, not for profit or other organizations) the following is required: Complete and submit *Questionnaire for Applicants/Owners which are Entities* (form 17-8295) with the application. For more information go to Canada Life™ *RepNet* under Forms & Procedures > Compliance	For **all** non-registered deposits of $100,000 or more (new issue or additional premiums) to an individual or jointly owned policy: Complete a PEFP Determination (form 17-8294) for each owner/contributor and forward to Head Office T424.
LIVING BENEFITS	**Beneficial owner**	**PEFP**
All Canada Life™ critical illness and disability insurance products	Living benefits products are considered low-risk and there are no additional requirements.	n/a

Identification of a third party individual form

When a third party is being added to a non-registered policy after it has been established, the third party must complete an *Identification of a third party individual form* (46-8708).

The Identification of a third party form must accompany all other required third party documentation when it is submitted to Head Office for processing

If there is more than one third party, use a separate form to record the information for each additional third party.

Appendix E - Process for reporting suspicious transactions and attempted suspicious transactions

User ID and password

Procedure

For more information, see: http://www.fintrac-canafe.gc.ca/reporting-declaration/1-eng.asp

Section 5 - Declarations of suspicious transactions and suspicious attempted transactions

When reporting a suspicious transaction to FINTRAC, a keep a copy of the report must be kept and will be filed here..

Section 6 - Training

Training program
Initial and ongoing:

Action plan 2020 - 2021

Training material and proofs of training

Additional information

Included here are emails, brochures, or documents relating to the compliance program for the fight against money laundering and terrorist financing.