Canadian Life
and Health Insurance
Association Inc.

Association canadienne
des compagnies d'assurances
de personnes inc.

GUIDANCE MANUAL

to

COMBAT

MONEY LAUNDERING

and

TERRORIST ACTIVITY FINANCING

This document has been designed to assist life insurance agents and brokers in complying with their legal obligations under Canada's anti-money laundering and anti-terrorist financing regime.

Revised July 28, 2008

TABLE OF CONTENTS

This document has been designed to assist life insurance agents and brokers in complying with their legal obligations under Canada's anti-money laundering and anti-terrorist financing regime.

GUIDANCE MANUAL FOR COMPLIANCE WITH CANADA'S ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING REGIME

1. Introduction

The purpose of this guidance manual is to provide you with an overview of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the *Act*) and the regulations, to assist you in developing a "knowledge base" from which you can exercise your judgment in carrying out your obligation to report suspicious activity related to a money laundering or terrorist activity financing offence.

The *Act* was passed on June 29, 2000. The *Act* was amended in December 2001 to include provisions dealing with the financing of terrorism and amended further in December 2006. The regulations have been amended and most of them will be in effect as of June 23, 2008. The legislation's intent is to strengthen Canada's efforts in the fight against transnational crime - specifically money laundering and the financing of terrorist activities.

The *Act* makes it mandatory for various individuals and entities, including life insurance agents and brokers, to report a variety of transactions to the *Financial Transactions and Reports Analysis Centre of Canada* (FINTRAC). The mandatory reporting is designed to assist in the detection and deterrence of money laundering and terrorist financing activities as well as to facilitate the investigation and prosecution of money laundering and terrorist activity financing offences.

1.1 What is money laundering

Money laundering is defined as "any act or attempted act to disguise the source of money or assets derived from criminal activity." Essentially, it is the process where 'dirty money' is transformed into 'clean money'.

Under Canadian law, a money laundering offence involves concealing or converting property or the proceeds of property (e.g., money), knowing or believing that the property or proceeds were derived from the commission of another offence (known as ***a predicate*** offence).

Predicate offences are not limited to the drug dealing offences commonly associated with money laundering. Predicate offences also include:

- Bribery of judicial officers
- Child pornography
- Breach of trust by a public officer
- Forgery
- Keeping a common bawdy house
- Procuring juvenile prostitution
- Theft
- Extortion
- Frauds on the government
- Corrupting morals
- Keeping gaming or betting house
- Betting, pool-selling, and bookmaking
- Murder
- Robbery
- Secret commissions
- Fraudulent manipulation of stock exchange transactions
- Possessing and/or uttering counterfeit money
- Fraud

1.2 Stages of money laundering

The process of money laundering is ongoing. Dirty money is constantly being introduced into the financial system in an effort to clean it. There are three recognized stages in the money laundering cycle:

- **Placement** is the initial stage in which money from criminal activities is placed in financial institutions. One of the most common methods of placement is **structuring-** breaking up currency transactions into portions that fall below the reporting threshold for the specific purpose of avoiding reporting or record

keeping requirements. Because most life insurance companies in Canada do not accept cash payments, you should be on the look out for cash equivalents, such as money orders or traveller's cheques.

- **Layering** is typically the second stage where the process of conducting a complex series of financial transactions is executed with the purpose of hiding the origin of money from criminal activity and hindering any attempt to trace the funds. This stage can consist of multiple securities trades, purchases of financial products such as life insurance or annuities, mortgages, cross-border transactions and wire transfers.
- **Integration** is the final stage. It involves placing the laundered proceeds of crime back in the economy to create the perception of legitimacy. For example, the money launderer becomes the beneficial owner of a legitimate business enterprise. In outward appearance it is a normal commercial entity. In reality, its whole operation is based on criminal money.

These stages can occur simultaneously, separately, or can overlap.

1.3 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.

1.4 What is terrorist activity financing

Under Canadian law, terrorist activity financing is when you knowingly collect or provide property, such as funds, either directly or indirectly, to terrorists. This includes inviting someone else to provide property for this purpose. It also includes the use or possession of property to facilitate or carry out terrorist activities.

Terrorists need financial support to carry out terrorist activities and achieve their goals. In this respect, there is little difference between terrorists and other criminals in their use of the financial system. A successful terrorist group, much like a criminal organization, is one that is able to build and maintain an effective financial infrastructure. For this, it must develop sources of funding and means of obscuring the links between those sources and the activities the funds support. It needs to find a way to make sure that the funds are available and can be used to get whatever goods or services needed to commit terrorist acts.

The fundamental aim of terrorist activity financing is to obtain resources to support terrorist activities. The funds needed to mount terrorist attacks are not always large and the associated transactions are not necessarily complex.

1.5 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.

1.6 How big is the problem and why is it important

Since money laundering and the criminal activities that it attempts to conceal are hidden, it is difficult to determine how widespread money laundering is throughout the world. Nevertheless, there is a consensus that the Canadian government should pay attention to money laundering and terrorist activity financing. Drug trafficking - considered to be the source of much of the money laundered through Canada - is believed to be a business earning multi-billion dollar amounts per year. Economic crimes such as fraud are also thought to be widespread in Canada. If money is laundered through life insurance agents and brokers, the reputation, and even the integrity, of the industry could be ruined.

1.7 Who is covered by this legislation

The *Act* applies to the following individuals and entities:

- Life insurance agents and brokers
- Life insurance companies
- Deposit-taking institutions
- Securities dealers - including portfolio managers and investment counselors
- Foreign exchange dealers
- Money services businesses
- Accountants and accounting firms
- Real estate brokers or sales representatives
- Casinos
- Agents of the crown or provinces that sell money orders or accept deposits from the public
- Employees of any of the above

Financial planners are also covered under the Act as securities dealers provided they are licensed to sell securities of any type (i.e., mutual funds, etc.)

2. FINTRAC

2.1 What is FINTRAC

The *Financial Transactions and Reports Analysis Centre of Canada* (FINTRAC), often referred to as "the Centre" in the *Act*, was established as an independent financial intelligence unit. FINTRAC will collect and coordinate the data it receives in order to facilitate more effective and efficient recognition of money laundering and/or terrorist activity financing as well as conducting its own internal research and obtaining information from other international sources. It operates independently from law enforcement agencies (e.g., the RCMP) even though part of its mandate is to assist in the detection and deterrence of money laundering and the financing of terrorist activity in Canada and around the world.

FINTRAC also has the primary responsibility to ensure reporting entities, such as life insurance agents and brokers, comply with Part 1 of the *Act* and its requirements. Subsequently, FINTRAC also has the authority to inquire into your business and examine your records to ensure compliance with the *Act.* Part of FINTRAC's mandate also includes increasing the public's awareness and understanding of money laundering and it will issue periodic reports on the usefulness of information it has received.

2.2 What does FINTRAC do with the information reported

If FINTRAC determines, based on its analysis and assessment, that there are reasonable grounds to suspect that the information reported would be relevant to the investigation or prosecution of a money laundering or terrorist activity financing offence, it will disclose ***designated information*** only to the appropriate police force.

If the police force wants more information than what FINTRAC has provided, it must obtain a court order directing the release of further information.

2.3 Who may FINTRAC disclose information to

In addition to the appropriate police force, FINTRAC may also disclose this same ***designated information*** to three other government agencies provided key conditions have been met. First, FINTRAC must determine that there **are reasonable grounds to suspect** that there is designated information that would be relevant to investigating or prosecuting a money laundering or terrorist activity financing offence and second, there is a determination of other criteria. Some of the other government agencies and some examples of the additional criteria that must be met are:

- **Canada Revenue Agency (CRA) -** if FINTRAC also determines that information is relevant to an offence of evading or attempting to evade paying taxes or duties imposed under an Act of Parliament administered by the Minister of National Revenue;

- **Canadian Security Intelligence Service (CSIS) -** if FINTRAC also determines that the information is relevant to threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act;* and

- **Canada Border Services Agency**, if FINTRAC also determines that the information is relevant to determining whether a person is a person described in sections 34 to 42 of the *Immigration and Refugee Protection Act* (the IMRPA) or is relevant to an offence under any of sections 117 to 119, 126 or 127 of the IMPRA.

FINTRAC may also disclose the designated information to other Financial Intelligence Units (FIU) where an information-sharing agreement is in place called "Memorandum of Understanding" (MOU).

2.4 Protection of privacy

The *Act* requires FINTRAC to respect individual privacy and to protect confidential information.
Some of the safeguards intended to protect the privacy of individuals are:

- Independence of FINTRAC from law enforcement and other government agencies entitled to receive information;

- Significant criminal penalties for unauthorized use or disclosure of personal information obtained by FINTRAC;

- That only limited ***designated information*** may be disclosed to law enforcement and only once FINTRAC has determined that there are reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering offence or a terrorist activity financing offence;

- The requirement that certain designated law enforcement and government agencies have to get a Production Order to obtain more than the ***designated information***; and

- The fact that FINTRAC is subject to the federal *Privacy Act.*

2.5 FINTRAC's authority under Part 1 of the Act

The *Act* authorizes FINTRAC to enter, at any reasonable time, any individual's or entity's business premises without a warrant. The only time a warrant may be required is when the individual's or entity's business premises are in a dwelling house. FINTRAC may not enter the dwelling house without the consent of the occupant except under the authority of a warrant issued under the *Act*.

The owner or person in charge of the business premises (including dwelling-house) and every person found there are required to give the authorized person all reasonable assistance to enable them to carry out their responsibilities. They are also required to furnish them with any information with respect to the *Act*.

A failure to assist a compliance officer (authorized person) in their efforts could, upon conviction, lead to up to five years imprisonment and/or a fine of $500,000.

2.6 FINTRAC's approach to compliance monitoring

FINTRAC states that it favours a co-operative approach to monitoring. The emphasis will be on working with life insurance agents and brokers to achieve compliance with the *Act* and regulations. As a general rule, when compliance issues are identified, FINTRAC will work with the life insurance agents and brokers in a constructive manner to find reasonable solutions. If these efforts are not successful or the breach is particularly egregious, FINTRAC may refer non-compliance cases to the appropriate law enforcement agencies.

3. Mandatory Compliance Regime

All individuals and entities covered under the *Act* are required to have a compliance regime. The compliance regime is intended to ensure you comply with all your obligations under the *Act.* Although you may never have to file a report, you will still have to put a compliance regime in place. The compliance regime is statutorily required - it is not an option. This manual may be used for your policies and procedures and should be customized to suit your practice if necessary.

The following five requirements must be met:

(i) the appointment of an individual (the compliance officer) who is to be responsible for the implementation of the regime. A sole practitioner may serve as the compliance officer;

(ii) the development and application of compliance policies and procedures. These policies and procedures have to be written and kept up to date. If you are an entity, they also have to be approved by a senior officer.

(iii) an assessment and documentation of risks related to money laundering and terrorist activity financing which assesses the risk of a money laundering offence or a terrorist activity financing offence. Where there is a high risk, special measures must be taken for identifying clients, keeping records and monitoring financial transactions in respect of the activities that pose the high risk;

(iv) a review, as often as is necessary, but at least every two years, of those policies and procedures to test their effectiveness, to be conducted by an internal or external auditor, where the person or entity has one, **or by the person or entity itself, where it does not have an internal or external auditor**; and

(v) if you have employees or agents or any other individuals authorized to act on your behalf, the implementation of an on-going compliance training program is required for them and it has to be in writing and maintained.

Implementation of a compliance regime is a requirement as well as a good business practice for anyone subject to the *Act* and regulations. A well-designed, applied, and monitored regime will provide a solid foundation for compliance with the legislation. FINTRAC recognizes that not all individuals or entities operate under the same circumstances, hence compliance regimes should be tailored to fit individual and entity needs and should consider the nature, size, and complexity of operations. Although there is this view of "flexibility", your program has to contain all five elements described above.

3.1 Appointment of compliance officer

The appointed compliance officer should have the authority and the resources necessary to discharge his/her responsibility effectively. Depending on the type of business, the compliance officer should report to the Board of Directors or senior management or to the owner or chief operator. You can also appoint yourself if your business is small. The implication is that the compliance officer needs to be a senior person in the business.

To ensure consistent and ongoing attention to the compliance regime, the compliance officer may choose to delegate certain duties to other employees. For example, you may delegate an individual in your office or another office to ensure that compliance procedures are properly implemented at your location or other location, if any. Even though you may wish to delegate some of these duties, the compliance officer remains responsible for the entity's overall compliance regime.

Individuals who are subject to the *Act* may appoint themselves as "compliance officer" or may choose to appoint another individual to help them implement the compliance regime. You should take care if someone asks you to be their compliance officer and you should also make sure the person you appoint is aware of their potential liabilities.

The *Act* covers life insurance agents and brokers as a profession - as individuals, as firms or members of firms and as partners in a partnership. This means individual practitioners in a firm or partnership will be responsible to make sure that their reporting obligations are met when it relates to any life insurance transaction they may be involved with. You may choose to have a compliance officer for the firm or partnership as a whole, but you are ultimately responsible for your individual responsibilities so you will want to make sure your obligations are being met.

3.2 Establishing compliance policies and procedures

An effective compliance regime is a commitment by each life insurance agent and broker to institute policies and procedures to prevent, detect, and address non-compliance with the *Act* and the regulations. The formality of the policies and procedures will depend on the degree of detail, specificity and formality of the regime, the complexity of the issues and transactions that you are involved in or will be involved in as well as the risk of exposure to money laundering and terrorist activity financing.

The policies and procedures should provide you and/or your personnel with enough information to properly process and complete a transaction. They should also provide a clear definition of roles and responsibilities for identifying reportable transactions, record keeping, record retention, ascertaining identity, exceptions, and completing and filing of reports.

You should consider what is necessary to ensure compliance with these requirements when assessing what specific policies and procedures should be implemented. The scope of policies and procedures will vary depending on the type and size of business you have. The policies and procedures for some may be less formal and simpler than those of others. What is important is that the policies and procedures are communicated, understood, and adhered to by you and all employees and staff.

Foreign subsidiaries and foreign branches in countries that are not members of the Financial Action Task Force must develop and apply policies and procedures regarding identity verification, record keeping and having a compliance program when the laws of the country permit it. Where the laws do not permit it, foreign subsidiaries must keep and retain a record of that fact in accordance with regulations.

3.3 Assessment and documentation of risks

- You must take a risk-based approach (RBA) to assessing and documenting risks related to money laundering and terrorist activity financing. You have to assess and document the risks by considering the following factors:

- your products and services and the delivery channels through which you offer them;
- the geographic locations where you conduct your activities and the geographic locations of your clients;
- other relevant factors related to your business; and
- your clients and the business relationships you have with them.

Keeping client identification is discussed under Section 9, Required Written Records.

If you consider the risk of a money laundering offence or a terrorist activity financing offence to be high, the risk has to be mitigated by adopting prescribed special measures for identifying clients, keeping records

and monitoring such life insurance transactions. The special measures that are required to be taken when the risk is high include the development and application of written policies and procedures for:

(*a*) taking reasonable measures to keep client identification information up to date;
(*b*) taking reasonable measures to conduct ongoing monitoring for the purpose of detecting transactions that are required to be reported to FINTRAC; and
(*c*) mitigating the risks identified.

3.4 Review of compliance policies and procedures

The *Act* calls for a mandatory review of the policies and procedures program. The review allows you to monitor the effectiveness of your compliance regime and evaluate the need to modify existing policies and procedures if necessary or implement new ones.

The compliance review should be conducted as often as necessary but must be carried out every two years. Some factors to consider that would prompt a need for a review are changes in the legislation, non-compliance issues, or new services and products being offered beyond life insurance.

The review must be conducted by either an internal or external auditor. If you do not have an internal or external auditor, you can do a "self-review" or have another outside party conduct the review. Whenever possible, the review should be conducted by an individual who is independent of the reporting, record keeping, and compliance monitoring so as to maintain objectivity.

Within thirty (30) days after the assessment, the following is required to be reported in writing to a senior officer:
(*a*) the findings of the review;
(*b*) any updates made to the policies and procedures within the reporting period; and
(*c*) the status of the implementation of the updates to those policies and procedures.

While not specifically required under the *Act*, it would be good business practice to document the scope and results of the review. Deficiencies and weaknesses that appear should be identified and reported to the senior management. The report should also include a request for a response indicating corrective measures and follow-up actions as well as a time-line for implementing such actions.

3.5 Ongoing compliance training

The success of a compliance regime is highly dependent on adherence. Only when you and/or your staff are made aware of the requirements and responsibilities will you and/or they be able to contribute to the program. On-going training is essential to maintaining a sound compliance regime. All individuals should be generally familiar with the legislation and regulations and should receive training in areas directly affecting their responsibilities. They must also be trained in policies and procedures the entity or individual adopts to ensure compliance with legal obligations.

Periodic training will help ensure adherence to policies and procedures. The method of training may vary greatly depending on your business' size, time requirements, and the complexity of the subject matter.

When assessing training needs, individuals and entities subject to the *Act* should consider the following elements:

Legislative and regulatory requirements and related liabilities - the training should provide an understanding of the legislative and regulatory requirements as well as the liabilities under the *Act* and applicable regulations;

Policies and procedures - the training should provide awareness of the internal policies and procedures for deterring and detecting money laundering that are associated with the job. It should also provide a concrete understanding of responsibilities;

Background information on money laundering and terrorist activity financing - any training program should include some background information on money laundering and terrorist activity financing to ensure that money laundering and terrorist activity financing are understood, why criminals choose to launder money, and how the process usually works.

For more information on creating a compliance regime, visit www.fintrac.gc.ca and refer to Guideline 4 – *Implementation of a Compliance Regime.*

4. 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" under the legislation.

5. Suspicious Transaction or Attempted Transaction Report (STATR)

The *Act* requires you to submit a Suspicious Transaction or Attempted Transaction Report (STATR) if you 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 you, or your staff, to exercise judgment.

The key questions for many are going to be, "*What constitutes a suspicious transaction or attempted transaction?*" and "*What are reasonable grounds?*" There is no easy answer to either of these questions. It is expected that through training (which is required under the *Act)* and with the assistance of this guidance manual, you will develop the judgment necessary to answer these key questions for yourself and thereby fulfill your legal obligations under the *Act.*

There is no minimum dollar threshold for reporting suspicious transactions or attempted transactions.

Some important factors to understand concerning your obligation to report a suspicious transaction or attempted transaction under the *Act* are:

- You are required to take reasonable measures to ascertain the identity of the person with whom the suspicious transaction or attempted transaction is being or has been conducted, unless you believe it would inform the person that the transaction or attempted transaction and related information is being or would be reported.

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

5.1 Identifying suspicious transactions or attempted transactions

When looking at a transaction or attempted transaction with a view towards deciding whether it is suspiciously related to a money laundering or terrorist activity financing offence, remember that *behaviour* is suspicious, not people.

It is the consideration of many factors which will lead you to conclude that there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering or terrorist acivity financing offence. You must look at the overall picture and consider some of the following factors:

- your knowledge of the client,
- your knowledge of client's industry,
- in the context of the transaction; is this normal,

- your 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 you consider it normal for a client to buy a whole life policy based on a needs analysis? The answer is probably yes. Would you consider it normal for a whole life policy buyer to be more interested in early redemption features than financial security needs? Probably not. As you 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.

5.2 Indicators of suspicious transactions or attempted transactions- general

The following is a sample of some general indicators that might lead a life insurance agent or broker to suspect that a transaction or attempted 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.

5.3 Indicators of suspicious transactions or attempted transactions - industry specific

The following is a sample of some industry specific indicators that might lead you 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 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 unfavourable 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.*

5.4 Reporting timelines for STATR

You have thirty (30) days, from the date on which you have reasonable grounds to suspect that the transaction or attempted transaction is related to a money laundering or terrorist activity financing offence to file your 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. You are not permitted to tell the client that you have made a report.

FINTRAC will send you an acknowledgement message when your report has been received electronically. This will include the date and time your report was received and a FINTRAC-generated identification number. If your report contains incomplete information, FINTRAC may contact you by phone, or you 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, your obligation to report is not considered fulfilled unless the report is complete.

5.5 Liability in relation to reporting STATR to FINTRAC

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, you 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.

5.6 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, you are prohibited by law to tell the client that you 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.*

5.7 Copy of STATR

Every person or entity who submits a STATR to FINTRAC, must keep a copy of the report.

6. Large Cash Transaction Report (LCTR)

Given the no cash policy of most, if not all, life insurance companies, the large cash transaction reporting obligation should be minimal.

You have to send a Large Cash Transaction Report (LCTR) to FINTRAC in either of the following situations:

- You receive an amount of $10,000 or more in cash in the course of a single transaction; or

- You receive 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, you have to make a LCTR if you know the transactions were made within 24 consecutive hours of each other by or on behalf of the same individual or entity.

6.1 Conditions for reporting large cash transactions

The conditions for reporting a large cash transaction are that you received a $10,000 cash amount in Canadian dollars or its equivalent in any foreign currency in respect of a transaction. Alternatively, if you know that two or more transactions are conducted by or on behalf of the same person or entity within a twenty-four hour period and they total $10,000 or more, they are to be treated as one transaction and are reportable as well.

6.2 Reporting timelines for LCTR

You have to send LCTRs to FINTRAC within 15 days after the transaction.

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

This process must be completed within the time period because your obligation to report is not considered fulfilled unless the report is complete.

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.*

7. Terrorist Group or Listed Person Property Report

7.1 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 traveller'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.*

7.2 Reporting under the *Act*

Every life insurance agent and broker is subject to the *Act* and the reporting of terrorist property.

As a "reporting entity", you have a legal obligation to send a terrorist property report to FINTRAC if you have property in your possession or control that you **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.*

7.3 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 you are a reporting entity under the *Act* or not and you do not have to be involved in any life insurance transactions before you are subject to the *Criminal Code* requirements.

The *Criminal Code* requires you to disclose to the RCMP and CSIS the existence of property in your possession or control that you **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 you have property in your possession or control that you ***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, you 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 you 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, you are to remove yourself from any involvement.

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

7.4 Reporting scenarios

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

Scenario 1 - If you ***do not know*** that the property in your possession or control is terrorist property and you

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 you ***do not know*** that the property in your possession or control is terrorist property but ***you 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 you will have to file *a* ***Suspicious Transaction or Attempted Transaction Report*** regarding such property**.**

Scenario 3 - If you have property in your possession or control that you ***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 you have been involved in a life insurance transaction, you 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 you have property in your possession or control that you ***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 you have not been involved in a life insurance transaction, you must disclose it to the RCMP and CSIS under the *Criminal Code.*

8. Making Reports to FINTRAC

8.1 Electronic reporting

You must submit all reports electronically, if you 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.

8.2 Report acknowledgement and correction requests

FINTRAC will send you an acknowledgement message when your report has been received electronically. This will include the date and time your report was received and a FINTRAC-generated identification number. Keep this information for your records.

If your report contains incomplete information, FINTRAC may notify you. The notification will indicate the date and time your 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. Your obligation to report will not be fulfilled until you send the **completed** report to FINTRAC. In light of this 30-day requirement, you should ensure that your policies and procedures call for the reports to be made as quickly as possible to leave you enough time to respond to any correction requests.

8.3 Paper reporting

Under the *Act,* you are required to report electronically to FINTRAC if you have the capability. If you do not have the technical capability to report electronically or you have to file a Terrorist Group and Listed Person Property Report, you must submit paper reports to FINTRAC. The following forms can be accessed from FINTRAC's website and printed at your office or local library, or other public place with Internet access or call 1-866-346-8722 for a copy to be faxed or mailed to you.

- 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, it would be preferable if paper reports were completed using word-processing equipment or a typewriter. 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 you any acknowledgement when a paper report has been received.

8.4 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 you to make a reasonable effort to get the information. The information that is required to be provided includes:

- Information about the reporting entity (you).
- 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 your reasons for suspicion and if you 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 you 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 your records you can leave the applicable LCTR field blank.

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

9. Required Written Records

Pursuant to the regulations under the *Act*, as a “reporting entity”, i.e., a life insurance agent or broker, you are required to keep certain records, namely large cash transaction and client information records. Other records that you may be required to keep, depending on the situation, may include records related to beneficial ownership, not-for-profit organizations, third party determinations, and politically exposed foreign persons.

9.1 Large cash transaction record

The requirements are:

- Prepare a large cash transaction record in respect of every amount in cash of $10,000 or more that is received in the course of a single transaction, unless the cash is received from a financial entity (such as a bank, credit union, caisse populaire or trust company) or public body.
- Ascertain the identity of the individuals involved in the transaction at the time of the transaction.
- Take reasonable measures to determine whether the individual who in fact gives the cash in respect of which the record is being made is acting on behalf of a third party.
- Prepare and retain a third party disclosure statement signed by the client if they are acting on behalf of a third party.
- Where you are not able to determine if the client is acting on behalf of a third party but there are reasonable grounds to suspect that the client is acting on behalf of a third party, prepare and retain a third party disclosure statement signed by the client stating that they are not acting on behalf of a third party.

* Please note: the client signature on the form is not a requirement under the *Act*, it is a suggested industry practice. See Section 9.5, Third party determination record (below).

There is no standard format or template for the large cash transaction record. You are to design one yourself that will include the required information. The information required is specified in detail in the regulations. The information required in the large cash transaction record includes the following:

- The name of the individual who in fact gives the amount (cash).
- The address and date of birth of the individual and the nature of their principal business or occupation.
- The date and nature of the transaction.
- The number of any account that is affected by the transaction as well as the type of account, the name of any person or entity that holds/owns the account, and the currency in which the account transactions are conducted.
- The purpose and details of the transaction, including other persons or entities involved and the type of transaction (such as cash, electronic funds transfer, deposit, currency exchange, or the purchase or cashing of a cheque, money order, travellers' cheque or banker's draft).
- Whether the cash is received in person, by mail, or in any other way.
- The amount and currency received.

It is important to remember that the ***large cash transaction record*** is different from the ***large cash transaction report*** (LCTR). Although there is some overlap of information required in each of these reports/records, there are differences. As such, the filing of a LCTR is not a substitute for having to also maintain the ***large cash transaction record.*** Keeping a copy of the LCTR that was submitted to FINTRAC can be used as large cash transaction record if all of the information for the record is included.

9.2 Client information record

If your client pays you $10,000 or more for an annuity or a life insurance policy, over the duration of the annuity or policy, you have to keep a client information record. This has to be kept no matter how the client paid for the annuity or policy, whether or not it was in cash.

For an individual - You must ascertain and record your 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. 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 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 you have reasonable grounds to believe that another life insurance company, broker or agent has confirmed the individual's identity, you do not have to confirm his/her identity again unless you 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 licence;
- provincial health insurance card (where allowed);
- passport; or
- any similar record other than the individual's social insurance number.

If you 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 following information:

- if you used a document used to confirm the individual's identity, the type of identification document used, its reference number and its place of issue;
- if you used a cleared cheque to confirm the individual's identity, the name of the financial entity and the account number of the account on which the cheque was drawn;
- if you confirmed the individual's identity by confirming that the individual holds an account with a financial entity, the name of the financial entity, the account number and the date of confirmation;
- if you use an identification product to confirm the individual's identity, the name of the identification product, the name of the entity offering the product, the search reference number, and the date the product was used to ascertain the individual's identity;
- if you are consulting a credit file kept by an entity in respect of the individual to ascertain the individual's identity, the name of the entity and the date of the consultation;
- if you use an attestation signed by a commissioner of oaths in Canada or a guarantor in Canada to ascertain the individual's identity, the attestation;

See Section 9.5, Third party determination record (below).

For a corporation -You 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, you do not have to ascertain the names of the corporation's directors.

See Section 9.3, Beneficial owners record, Section 9.4, Not-for-profit organization record, and Section 9.5, Third party determination record (below).

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

See Section 9.3, Beneficial owners record, Section 9.4, Not-for-profit organization record, and Section 9.5, Third party determination record (below).

In a **non-face-to-face situation**, you (or the insurer) have two options for ascertaining identity:

OPTION 1:

The client identity can be ascertained by:

- obtaining the individual's name, address and date of birth; and
- confirming that one of the following entities has identified the individual by referring to the individual's birth certificate; driver's licence; provincial health insurance card (where allowed); passport; or any similar record other than the individual's social insurance number:
  - (a) an entity affiliated with you;
  - (b) an entity affiliated with you that carries on activities outside Canada that are similar to you; or
  - (c) an entity that is a member of the same association - being a central cooperative credit society within the meaning of section 2 of the Cooperative Credit Association Act; and
- verifying that the individual's name, address and date of birth corresponds with the information provided by the affiliated entity or the entity that is a member of the same association.

(An entity is affiliated with you if you wholly-own it or it wholly-owns you, or you are both wholly-owned by the same entity.)

OPTION 2:

The client identity can be ascertained by using any of the following combination of methods as long as the individual's information obtained by the two methods is consistent with each other and is consistent with your records:

- method 1 and 3;
- method 1 and 4;
- method 1 and 5;
- method 2 and 3;
- method 2 and 4;
- method 2 and 5;
- method 3 and 4; or
- method 3 and 5.

The five different methods are the following:

1) IDENTIFICATION PRODUCT METHOD - Refer to an independent and reliable identification product that is based on personal information in respect of the individual and a Canadian credit history of the individual of at least six month’s duration.

2) CREDIT FILE METHOD - Confirm, after obtaining authorization from the individual, their name, address and date of birth by referring to a credit file in respect of that individual in Canada that has been in existence for at least six months.

3) ATTESTATION METHOD - Obtain an attestation from a commissioner of oaths in Canada, or a guarantor in Canada, that they have seen the individual's birth certificate, driver's licence, provincial health insurance card (if not prohibited by the applicable provincial law) passport or other similar document. The attestation must be produced on a legible photocopy of the document (if such use of the document is not prohibited by the applicable provincial law) and must include (*a*) the name, profession and address of the person providing the attestation; (*b*) the signature of the person providing the attestation; and (*c*) the type and number of the identifying document provided by the individual.

4) CLEARED CHEQUE METHOD - Confirming that a cheque drawn by the individual on a deposit account of a financial entity, other than an account that is an exception to ascertaining identity, has been cleared.

5) CONFIRMATION OF DEPOSIT ACCOUNT METHOD - Confirm that the individual has a deposit account with a financial entity, other than an account that is an exception to ascertaining identity.

Exceptions to record-keeping and ascertaining client identity - there are several exceptions that are specifically set out under section 62 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations.*

For instance, you do **not** have to keep a client information record for a policy that is an exempt policy (i.e., a policy issued mainly for insurance protection and not investment purposes as defined in subsection 306(1) of the *Income Tax Regulations*). Likewise, you do **not** have to keep a client information record for a group life insurance policy that does not provide for a cash surrender value or a savings component. For a group plan account, a life insurance company, broker or agent is not required to ascertain the identity of any individual member or determine whether they are a politically exposed foreign person, if the member's contributions are made by the sponsor of the plan or by payroll deductions and the existence of the plan sponsor has been confirmed.

9.3 Beneficial owners record

If your client is a corporation, you must, at the time the existence of the corporation is confirmed, take reasonable measures to obtain and, if obtained, keep a record of the name and occupation of all directors of the corporation and the name, address and occupation of all persons who own or control, directly or indirectly, 25 per cent or more of the shares of the corporation.

If your client is not a corporation, you must, at the time the existence of the non-corporation entity is confirmed, take reason measures to obtain and, if obtained, keep a record of the name, address and occupation of all persons who own or control, directly or indirectly, 25 per cent or more of the non-corporation entity.

Where you are not able to obtain the information, you shall keep a record that indicates the reason why the information could not be obtained.

9.4 Not-for-profit organization record

Where your client is a not-for-profit organization, you shall keep a record that sets out, whether that entity is (*a*) a charity registered with the Canada Revenue Agency under the *Income Tax Act*; or (*b*) an organization, other than one referred to in paragraph (*a*), above, that solicits charitable financial donations from the public.

9.5 Third party determination record

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

- Where the third party is an individual, the third party's name, address, date of birth and the nature of the principal business or occupation of the third party.

- Where the third party is a person or entity other than an individual, the third party's name, address, and the nature of the principal business of the third party.

- 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.

9.6 Politically exposed foreign person record

You 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: (a) head of state or head of government; (*b*) member of the executive council of government or member of a legislature; (*c*) deputy minister or equivalent rank; (*d*) ambassador or attaché or counsellor of an ambassador; (*e*) military officer with a rank of general or above; (*f*) president of a state-owned company or a state-owned bank; (*g*) head of a government agency; (*h*) judge; (*i*) leader or president of a political party represented in a legislature; or(*j*) 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 (*a*) the person’s spouse or common-law partner; (*b*) a child of the person; (*c*) the person’s mother or father; (*d*) the mother or father of the person’s spouse or common-law partner; and (*e*) a child of the person’s mother or father.

Where it has been determined that a person is a PEFP, you 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.

Every life insurance broker or agent, unless dealing in reinsurance, shall keep a record of the following information when a PEFP transaction is reviewed: (*a*) the office or position in respect of which the person initiating the transaction is determined to be a politically exposed foreign person; (*b*) the source, if known, of the funds that are used for the transaction; (*c*) the date of the determination that the person is a politically exposed foreign person; (*d*) the name of the member of senior management who reviewed the transaction; and (*e*) the date the transaction was reviewed.

9.7 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 shall 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 you 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.

10. Offences, Penalties, Due Diligence, and Liability

The *Act* contains a number of different penalties for different offences. Failure to comply with the different requirements under the *Act* can lead to criminal charges against the reporting entity as well as any individual subject to the *Act* (this includes employees and staff of reporting entities).

The *Act* states that in prosecuting an offence for failure to file an STATR, LCTR, or Terrorist Group and Listed Person Property Report, it is sufficient proof of the offence to establish that an employee or agent of the accused committed it, whether or not the employee or agent is identified or has been prosecuted for the offence.

10.1 Penalties for non-compliance

The breaches for non-compliance and their respective maximum penalties are:

- Failure to file a Suspicious Transaction or Attempted Transaction Report (STATR) - up to 5 years in jail and/or a fine of $2,000,000 (s.75 of the *Act*);
- Failure to file a Large Cash Transaction Report (LCTR) - $500,000 for first offence and $1,000,000 for each subsequent offence (s.77 of the *Act*);
- Failure to file a Terrorist Group or Listed Person Property Report - up to 5 years in jail and/or a fine of up to $2,000,000 (s.75 of the *Act*);
- Failure to maintain a record of a large cash transaction - $500,000 for first offence and $1,000,000 for each subsequent offence (s.77 of the *Act*);
- Failure to retain required records - up to 5 years in jail and/or fine of $500,000 (s.74 of the *Act*);
- Failure to implement a compliance regime - up to 5 years in jail and/or a fine of $500,000 (s.74 of the *Act*);
- Disclosing the fact that an STATR has been made with the intent to prejudice a criminal investigation - up to 2 years in jail (s.76 of the *Act*); and
- Failure to assist in a compliance review - up to 5 years in jail and/or fine of $500,000 (s.74 of the *Act*).

Generally, these fines are not covered by errors and omissions insurance unless coverage is specifically mentioned.

Effective December 30, 2008, administrative monetary penalties may be applicable under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations* (the *AMPR*), such as:

- Failure to implement any of the five elements of the compliance regime - a fine of up to $100,000 for each one.

The *AMPR* specifies a range of penalties for each of the three types of violations. The three types of violations are minor, serious and very serious. The penalty can be up to $500,000 in the case of a very serious violation.

For more information on administrative monetary penalties, visit www.fintrac.gc.ca and refer to Guideline 4 – *Implementation of a Compliance Regime.*

10.2 Due diligence and other defences

There are several defences and protections contained in the *Act.*

- No person shall be found guilty of not reporting a suspicious transaction or attempted transaction, a large cash transaction or terrorist group or listed person property if they can show that they exercised due diligence to prevent its commission. According to case law, to establish due diligence a person must show that he/she acted under an honest belief in a state of facts which, if they had been as he/she believed them to be, would have rendered his/her involvement innocent, or if he/she took all reasonable steps to avoid the particular event. This makes the due diligence defence a legal requirement rather than a professional standard. As such, there is a very high onus to establish that you used due diligence to prevent the commission of the breach. At a minimum, part of establishing due diligence will include reviewing whether the required compliance regime was put in place and whether the employees and/or staff have been trained on an ongoing basis to ensure their awareness of their requirements under the *Act* and the entity's policies and procedures for making such reports.

- No criminal or civil proceedings lie against a person or an entity for making a report in good faith. The key here is that the report(s) had to be made in good faith. This is one of the reasons why you must list your reason for making the report (i.e., what made you suspicious).

10.3 Vicarious liability of officers/directors

If any person or entity covered under the *Act* commits an offence, any officer, director, or agent of the person or entity who directed, authorized, assented to, acquiesced in, or participated in its commission is a party to and guilty of the same offence. They will also be subject to the same punishment if convicted, regardless of whether or not the person or entity itself has been prosecuted or convicted. In simple terms, it means you can be found guilty of an offence under the *Act* even though your corporate entity or the corporation you work for has not been found guilty.

This ensures that responsibility and accountability for compliance rests with senior management. This significantly extends the law on who may be a party to a criminal offence. It is also not a very high burden when you consider that in prosecuting a failure to report, it is sufficient proof of the offence to establish that an employee or agent of the accused committed the offence, whether or not the employee or agent is identified or prosecuted.

11. Using This Manual as Your Policies and Procedures

I _____have read and accepted this document as my policies and procedures on _____.
(life insurance agent's/broker's name) (date)

DESCRIPTIVE SCENARIOS OF SUSPICIOUS LIFE INSURANCE TRANSACTIONS OR ATTEMPTED TRANSACTIONS

SCENARIO NO. 1 - NO PICTURE I.D.

Fact: A potential customer 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 customer 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.

SCENARIO NO. 2 - 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.

SCENARIO NO. 3 - HIGH RISK BUSINESSES

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.

SCENARIO NO. 4 - DISREGARD FOR MONETARY LOSSES

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.

SCENARIO NO. 5 - 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.

SCENARIO NO. 6 - KNOW YOU CUSTOMER

Fact: You have written an application for life insurance and the client provides payment to you in the form of eighteen money orders totalling $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.

SCENARIO NO. 7 - 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.

SCENARIO NO. 8 - 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.

SCENARIO NO. 9 - 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.

SCENARIO NO. 10 - 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.

SCENARIO NO. 11 - 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.

SCENARIO NO. 12 - 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.

SCENARIO NO. 13 - REPEATED BENEFICIARY CHANGES

Fact: You are contacted by a potential client who wants to buy life insurance with a 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.

SCENARIO NO. 14 - KNOWLEDGEABLE CUSTOMERS

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".

SCENARIO NO. 15 - SPECIAL FAVOURS OFFERING

Fact: While providing life insurance advice, the client offers you money, gratuities or unusual favours 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.

This comprehensive Guidance Manual to Combat Money Laundering and Terrorist Activity Financing will assist you with record-keeping and reporting requirements under the Act and regulations.