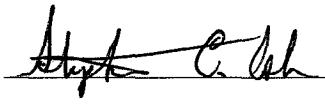
CAILBA ANTI-MONEY LAUNDERING AND ANTI-TERRORISM FINANCING COMPLIANCE PROGRAM

Effective Date:	**May 23, 2012**
Revised on:	**July 15, 2013**
Risk Assessment Date:	**Aug 12, 2013**
Self-Assessments/Reviews:	**Reviewed Annually**
Appointed Compliance Officer(s):	**STEPHEN ASH**
Signature of Senior Officer:	
Date:	**July 24, 2013**

This manual incorporates elements of both the FINTRAC 2008 Guidance Manual for Compliance with Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime and The Canadian Life and Health Insurance Association ("CLHIA") Guidance Manual to Combat Money Laundering and Terrorist Financing, revised July 28, 2008, which was created as an industry service and is intended for use by insurers' distribution partners.

TABLE OF CONTENTS

Appendices

What the Act Requires

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the "Act") requires Advisors adopt a Compliance Regime and comply with the Act. According to FINTRAC, "your compliance regime will have to be tailored to fit your own individual needs. It should reflect the nature, size and complexity of your operations."

The Act's 5 requirements include:

1. Assessing and documenting the money laundering and terrorist financing risks unique to our business.
2. Appointing a Compliance Officer.
3. Developing detailed, auditable compliance policies and procedures for reporting and record-keeping.
4. Ongoing review of the effectiveness of the compliance program through self-assessments and/or audits.
5. Compliance training for employees, agents or others acting on behalf of the MGA and a forward-looking *training plan*.

According to FINTRAC, in addition to whatever criminal penalties might apply to any situation, "failure to identify clients, keep records, monitor financial transactions and take mitigating measures in situations where risk of money laundering or terrorist financing is high could lead to an Administrative Monetary Penalty of up to $100,000." Clearly, adopting written policies and procedures provides some protection, but failure to actually *follow* those policies and procedures can leave an organization vulnerable.

The Act provides for a due diligence defense, but according to the CLHIA, "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 advisor is updated 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. "

The Act applies to life insurance brokers and agents, who are defined as "an individual or entity licensed provincially to carry on the business of arranging contracts of life insurance."

Appointment of Compliance Officer(s)

Under the Act, Compliance Officers are responsible for:

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

Under existing rules, the Compliance Officer may obtain the assistance of another person to manage the Firm's compliance responsibilities provided that this person has the necessary experience and skills and provided that this person's name and responsibilities are documented in the compliance program.

Semi-Annual Report of the Compliance Officer

The Compliance Officer will provide a written report to the Owner, which identifies any new initiatives undertaken, any compliance deficiencies identified in the period covered by the report, any corrective actions taken and any reports that were filed with FINTRAC.

Risk Assessment

According to FINTRAC "a risk-based approach (RBA), is a process that encompasses the following:

- the risk assessment of your business activities using certain factors;
- the risk-mitigation to implement controls to handle identified risks;
- keeping client identification and, if required for your sector, beneficial ownership information up to date; and
- the ongoing monitoring of financial transactions that pose higher risks."

Our risk assessment must be conducted as often as necessary but in no event less than once every two years. Our risk assessment focuses on:

Compliance Procedures (Risk Management and Mitigation)

Like all advisors, I could face legal, regulatory, financial and reputation consequences associated with fraud and market conduct abuses perpetrated by Producers or their customers. In many respects, the Producers with whom we contract are our customers or clients. In order to fulfill our contracts with our insurance suppliers, we take a number of steps to mitigate these risks, including procedures aimed at detecting and preventing fraud, including money laundering.

Risks and Controls

FINTRAC has indicated that some insurance *products* can be attractive to money launderers. In fact, product risk is the most important risk to consider in our business. Certain independent Producers and their *customers* who are intent on exploiting these products' advantages also pose risks. Insurers face these risks directly and we rely on their controls in addition to those we have implemented for higher risks.

Product risk controls: Insurers have embedded questions in applications and forms for high risk products and many insurers' transaction monitoring systems are designed to identify anomalies and unusual patterns.

Producer risk controls: All Producers with whom we do business are provincially licensed, which means they have been screened by a regulator, including criminal background checks. They have had to attain the necessary credentials in order to be able to sell insurance, which might serve as a barrier to entry for money launderers. Brokers are also directly subject to the requirements and penalties of the Act. Insurers and we screen these Producers prior to entering into contracts with them.

Best Practices:

We actively monitor the flow of business, looking for anomalies and patterns that might represent improper market conduct practices and fraud, including money laundering. We consider these to be powerful controls that minimize risks presented by the channel in which we do business.

Customer risk controls: Like insurers and Producers, we have implemented policies and procedures to capture and maintain customer identity information. See Written Records below.

New Business and Inforce Checklists/Prompts and Escalation

Our staff reviews applications and inforce changes in order to be able to submit them in good order to insurers. In the process, we also use these reviews as a way of monitoring Producer and customer activity in high risk products. Staff members are given instructions on when to escalate to a Compliance Officer.

Yearly training reinforces the reasons behind the monitoring and is intended to sensitize staff to unusual sales patterns and questionable policy changes.

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

Making Reports to Regulators

Immunity: No criminal or civil proceedings may be brought against us if we have made a report in good faith. Given the severe penalties for failing to make reports, the burden is on us to ensure that we discharge our obligations.

Suspicious Transaction or Attempted Transaction Report ("STATR") Rules:

We are required to submit a STATR if we have *reasonable grounds* to suspect that a transaction or *attempted* transaction that we identify in the course of our activities as Advisors is related to money laundering or terrorist activity financing offenses. There is no minimum dollar threshold. The report must be filed within 30 days of the date on which *reasonable grounds for suspicion* were identified.

We are also required to take *reasonable measures* to ascertain the identity of the person making or attempting the transaction unless we believe that by doing so this person would recognize that we are making a report. Since we do not interact directly with Producers' retail customers, any efforts we make to ascertain identity would likely have to be through the Producer. We are prohibited from disclosing to the Producer or the Producer's customer that we have filed a report. We are required to keep a copy of any STATRs we file.

Employees are considered to be "reporting entities" by FINTRAC for this purpose only. By reporting concerns to the Compliance Officer as soon as they are identified, the employee has discharged his or her duty.

STATRS must be filed electronically via FINTRAC's secure website at www.fintrac.gc.ca. The instructions and codes for making electronic reports are housed in a safe and secure location.

STATR Procedures:

According to FINTRAC, "as a general guide, a transaction may be connected to money laundering or terrorist activity financing when you think that it (or a group of transactions) raises questions or gives rise to discomfort, apprehension or mistrust." We instruct our staff to look for things that seem to be out of the normal and to trust their gut feelings in deciding when to escalate concerns.

1. If a review triggers concern about a transaction, escalate it immediately to the Compliance Officer. While the Compliance Officer should not discuss whether a STATR report will be or has been filed, he or she may contact the insurer(s) involved to consult regarding the transaction. The decision as to whether to file a STATR should not be discussed.
2. The Compliance Officer will immediately review to determine *whether* to report and *what* to report. As of the date that the Compliance Officer determines that reasonable grounds exist, we have 30 days to make any report. If inquiries through the Producer are required in order to reach the end customer, there is an enhanced likelihood that the customer would surmise that we were making a report. This must be taken into account each time a suspicious transaction is identified, particularly if there are concerns about whether the broker is involved.
3. Where a STATR has been filed, arrange to monitor policy level and customer level activity on any affected policies for which we have records.
4. Arrange to monitor the broker's book of business for some period of time.
5. Compliance Officer may flag policy/associated policy/customer/broker on our administrative system for monitoring and reporting or set up a manual process for monitoring.

Time is of the Essence. STATR reports and any follow up requests by FINTRAC must be filed with FINTRAC within 30 days of the detection of a fact that constitutes reasonable grounds. It is therefore of paramount importance that concerns be escalated to the Compliance Officer as soon as they arise. The Compliance Officer, in turn, must immediately consult the appropriate section of FINTRAC guidance and determine whether a report must be filed.

Large Cash Transaction Report ("LCTR") Rules:

A LCTR must be filed with FINTRAC if

- $10,000 or more in cash is received in a single transaction or
- two or more cash amounts totaling $10,000 or more are received within a consecutive 24-hour period from the same individual or on behalf of the same individual or entity.

LCTRs must be made filed electronically via FINTRAC's secure website at www.fintrac.gc.ca within 15 days after the transaction. The instructions and codes for making electronic reports are housed a safe and secure location.

LCTR Procedure:

Neither we nor our insurance suppliers accept cash. Therefore, the likelihood of having to make a LCTR is virtually nil. In the very unlikely event that accepted cash that triggered a need to report, we would file a report according to the rules.

1. If a customer *attempts* to pay for a policy with cash and the attempt meets the criteria described in the STATR Rules section above, a STATR most certainly should be filed.
2. Regardless of the size of an attempted cash payment, if the circumstances are in any way suspicious and trigger any red flags, the Compliance Officer must decide whether to file a report after also reviewing **www.**fintrac.gc.ca and Guideline 5 and Guideline 7 – Submitting Large Cash Transaction Reports to FINTRAC.
3. Compliance Officer may flag any customer/policy/associated policy/broker on our administrative system for monitoring and reports or set up a manual process for monitoring.
4. The Compliance Officer may consult with the affected insurer regarding the case, but should not discuss any decision about filing a STATR.
5. Other methods of payment accepted by our Agency are by Pre-authorized debit Pad, Personal and Corporate Chequing Account.

Terrorist Group or Listed Property Report Rules:

My company is a "reporting entity" with a legal obligation to send a terrorist property report to FINTRAC if we have property in our possession or control, including premium payments and insurance policies, that we (or an associated person) knows is owned or controlled by or on behalf of a terrorist group or listed person. According to FINTRAC, "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."

Additionally the Criminal Code of Canada requires each Canadian, regardless of where residing, to disclose to CSIS and the RCMP the existence of property in that person's possession or control that meets the criteria above.

If our company encounters any such circumstance, they may not complete or be involved in the transaction or attempted transaction. They must remove themselves from any involvement. Under the Criminal Code, the property must be frozen.

Terrorist Group or Listed Person Property Reports can only be paper filed as of the date of this manual.

Terrorist Group or Listed Property Report Procedure:

1. When an attempted or completed transaction is escalated by a staff member or Producer or is detected by the Compliance Officer, the Compliance Officer should immediately review, which contains detailed instructions to assist in determining *what*, if any, reports must be made and to *which* entities.
2. It is of utmost importance to interview the person who claims to know that he or she is in possession or control of terrorist property.
3. The Compliance Officer should consult the most current lists supplied by OSFI at http://www.ofi-bsif.gc.ca by referring to the "Terrorism Financing" link.
4. When an attempted transaction is detected, extra care must be taken to ensure that the property in question (most likely a premium payment, insurance policy, refund or payment of a benefit). Under the Criminal Code, it may have to be frozen.
5. If a *non-staff* licensed independent Producer notifies the MGA that he or she may be in possession of such property, the Producer is required to make the report.
6. The Compliance Officer should check with insurers as to their requirements for notification of this kind of report.

Written Records Required for Selling Producers and Insurers

Large Cash Transaction ("LCT") Record Rule:

An insurer and Producer must maintain large cash transaction records that include:

- the amount and currency of the cash received;
- the name, date of birth and address of the individual from whom you received the cash and that individual's principal business or occupation;
- the date of the transaction;

- the purpose, details and type of transaction (for example, the cash was used to put a deposit on a purchase of a life insurance policy, etc.), including whether any other individuals or entities were involved in the transaction;
- how the cash was received (for example, in person, by mail, by armoured car, or any other way); and
- if an account was affected by the transaction, include the following:
    - the number and type of any such account;
    - the full name of the client that holds the account; and
    - the currency in which the account's transactions are conducted.

Large Cash Transaction ("LCT") Record Procedure:

We and all of our insurance carriers have a "no cash" policy, which means the likelihood of a Producer contracted with us having to maintain this record is virtually nil.

1. If we learn that an attempt was made to pay by cash and the Compliance Officer considers this suspicious, we must file a STATR with FINTRAC.
2. If cash was actually received, we must file an LCTR.
3. The Producer and insurer must maintain any actual LCT record.
4. Retain a copy of any record submitted by the Producer.
5. Input information on our administrative system.
6. Compliance Officer may flag policy/associated policies/broker/customer on system for monitoring and reporting or set up a manual process for monitoring.

Client Information Records Rules:

For all non-exempt life and annuity policies where premiums paid over the life of the policy would reach $10,000 or more, an insurer and Producer need to verify client identity by referring to valid original documents within 30 days by creating a record that contains the client's name, address, date of birth and principal business or occupation. "Client" for group sales means the applicant.

Client Information Records Procedure:

We have verified that our insurance company suppliers have embedded client ID requirements in their applications and supporting material, where necessary.

1. Review applications/forms for good order.
2. Retain copy for administrative purposes, if the record is provided by the Producer.
3. Input information on our administrative system.
4. Compliance Officer may flag policy/associated policies/broker/customer for monitoring and reports or set up a manual process for monitoring.

Beneficial Owners Record Rules:

According to FINTRAC, "a client acting on behalf of an entity who is not aware of that entity's beneficial owners ...may lead you to consider that client as a higher risk."

Insurers and Producers are required to obtain (and for high risk clients they identify, update every two years) beneficial ownership information about certain entities. A beneficial owner is anyone who owns or controls, directly or indirectly, 25% or more of an entity. In that case, the name, address and occupation of all of the corporation's directors must be maintained.

Beneficial Owners Record Procedure:

Insurers have *generally* embedded beneficial owner identification requirements in their applications, but have not generally reached out for updates.

1. By keeping copies of applications for administrative purposes, we capture initial identification information if it is provided to us by the Producer.
2. We post a reminder on our website to update any necessary information.
3. If an insurer notifies us that it has identified high risk customers who trigger the requirement to update, we will notify the Producer of the requirement and follow up in an effort to ensure that it was fulfilled.
4. Where we become aware of a high risk customer, they will be subject to greater monitoring on our part.
5. Create record on our administrative system.
6. Compliance Officer may flag policy/associated policies/broker customer for monitoring and reporting or set up a manual process for monitoring.

Not-for-Profit Organization Record Rule:

Where a customer is a not-for-profit organization, Producers and insurers are required to keep a record that indicates whether the customer is a charity registered with CRA or a non-registered entity that solicits charitable financial donations.

According to FINTRAC, any transaction in which "the client is acting on behalf of a third party but does not know anything about the third party may lead you to consider that client as a higher risk."

Not-for-Profit Organization Record Procedure:

This information would likely be uncovered in the course of the Producer's client identity verification.

1. Verify that the application is in good order before passing it through to the insurer.
2. Retain a copy of the record if the Producer provides it.
3. Create record on the administrative system.
4. Compliance Officer may flag policy/associated policies/broker/customer for monitoring and reports or set up a manual process for monitoring.

Third Party Determination Record Rules:

Every reasonable effort must be made by a Producer and insurer to determine whether the owner of the policy is acting on behalf of a third party. If this situation is identified, a third party determination record must be created, which contains the name, address, DOB and principal business of the third party (if an individual) and all of the above except DOB (if an entity), along with the nature of the relationship between the owner and the third party. If there are suspicions regarding the involvement of a third party, a statement must be signed by the owner that they are not acting on behalf of a third party.

Third Party Determination Record Procedure:

Insurers cover off these requirements in their applications and processes. Typically, the Producer is required to ask about third party involvement on the application.

1. Review material submitted by the Producer for good order before passing it through to the insurer.
2. Retain copies for administrative reasons, if the Producer provides the record.
3. Create record on the administrative system.

4. Compliance Officer may flag policy/associated policies/broker/customer for monitoring and reports or set up a manual process for monitoring.

Politically Exposed Foreign Person ("PEFP") Record Rules:

Life insurers and Producers are required to take reasonable measures to determine whether anyone who makes a lump-sum payment of $100,000 or more for an immediate or deferred annuity or life insurance policy is a PEFP. The definitions of PEFP can be found in FINTRAC Guideline 9.6.

Where it has been determined that a person is a PEFP, the insurer and Producer must take reasonable measures to establish the source of the funds used for the transaction. Additionally, the transaction must be reviewed by a member of senior management within 14 days after the transaction.

Producers and insurers are required to keep a record of (a) the office or position that causes the person initiating the transaction to be considered a PEFP; (b) the source of funds, if known; (c) the date it was determined the person was a PEFP; (d) the name of the member of senior management who reviewed the transaction; and (e) the date the transaction was reviewed.

According to FINTRAC, any client known to be a PEFP should automatically be considered a higher risk.

Politically Exposed Foreign Person ("PEFP") Record Procedure:

Insurers generally cover off these requirements in their applications and processes. Typically, the Producer is required to ask about PEFP status on the application.

1. Review the material submitted by the Producer for good order before passing it through to the insurer.
2. If $100,000 or more has been received in a single payment, check to see that PEFP determination has been made.
3. Retain copies for administrative reasons if the Producer provides the record.
4. Create record on the administrative system.
5. Escalate to Compliance Officer, who may flag policy/policies/broker/customer for monitoring and reports or set up a manual process for monitoring.

Records Retention Requirement Rule:

Records must be maintained by insurers and Producers for 5 years from the day they were created or from the date of the last transaction. They must be in machine-readable form or in electronic form with a proper electronic signature. They must be provided to FINTRAC within 30 days after a request.

Records Retention Requirement Procedure:

Our company maintains records for administrative purposes in order to fulfill our obligations to insurers and Producers. We maintain whatever records are submitted by Producers and required by insurers in connection with the sale and service of policies. If FINTRAC were to make a request, we would respond by assisting the Producer and/or insurer in compiling records and would make available the records we maintain in our own systems and files. We will retain records for the period required.

FINTRAC'S Privacy Safeguards:

FINTRAC provides assurance that it has safeguards in place including

- independence from law enforcement and other agencies to which it is authorized to disclose information;
- criminal penalties for unauthorized use or disclosure of personal information under its control;
- the requirement that police get a court order to obtain further information from FINTRAC; and
- the application of the *Privacy Act* to FINTRAC.

Self-Assessments and Audits of Compliance Policies and Procedures

Rules:

We are required to review our policies and procedures at least every two years to test their effectiveness, taking into account changes in legislation or regulation, any non-compliance we find and any new services or products that have been introduced.

The review can be as sophisticated as a full-blown audit conducted by an outsider and as simple as a self-assessment performed by us or an outside party. It is highly recommended that the review be conducted by a person who is independent of reporting, record keeping, and compliance monitoring.

A written report must be delivered to a senior officer within thirty days following the completion of the assessment. The report must contain the findings and identify any updates to policies and procedures within the reporting period along with the status of implementation of these updates. FINTRAC suggests that the scope and any deficiencies or gaps be reported, with a request for a management response, action plan and timeline for implementation.

Failure to report to senior management within thirty days of a review could lead to an Administrative Monetary Penalty of up to $100,000.

Procedures:

FINTRAC and CLHIA guidance were consulted in preparing our review of our business. Our self-assessment fits our business needs and reflects the nature, size and complexity of our organization. Weaknesses, proposed corrective actions, a timeline for implementing such actions and any follow-up actions are noted. Any deficiencies are identified and reported to the principal(s). The results of this review are documented and kept on file.

From time to time, our program may be reviewed by external parties, with the results documented and reported within 30 days of the review to a senior manager for follow-up and corrective measures. The last such review is identified on the face page of this document. The results are kept on file.

Anti-Money Laundering and Anti-Terrorist Financing Training Program

Rules:

According to FINTRAC, "if you have employees, agents or other individuals authorized to act on your behalf, your compliance regime has to include training." Staff and management must be educated as to how their MGA and the industry are vulnerable to abuse by criminals laundering the proceeds of crime or by terrorists financing their activities. Examples of how brokers and MGAs can be used to launder illicit funds or fund terrorist activity should be included.

Finally, the advisor must be made aware that they cannot disclose that they have made a STATR, or disclose the contents of such a report, with the intent to prejudice a criminal investigation, and that there is immunity for making a report in good faith.

Procedure:

We have implemented and will continue to refine a training program for our staff. Producers have a formal regulatory obligation to have their own training and we require them to certify that they have received such training

At a minimum, we will annually review our compliance program and policies and procedures with staff, along with a presentation that covers any changes to law or internal processes, the relevant sections of FINTRAC guidance and any emerging typologies. New employees will be trained soon after they are hired. Our training events are noted on our Compliance Calendar.

Additional training will be made available on an ad hoc basis and can consist of posted material on our website generated by CLHIA, FINTRAC, Advocis, LIMRA on behalf of CAILBA, and other suppliers for use by Producers and staff. Programs designed and delivered by insurers and presentations we generate are also made available. Records of attendance at training are maintained in our files.

Penalties for Non-Compliance

"Failure to comply with the compliance regime, reporting, record keeping or client identification requirements can lead to criminal charges against a reporting entity. Conviction of failure to retain records could lead to up to five years imprisonment, to a fine of $500,000, or both. Alternatively, failure to keep records or identify clients can lead to an administrative monetary penalty. For more information on penalties, consult the Penalties for non-compliance section of FINTRAC's Web site (www.fintrac-canafe.gc.ca)." (FINTRAC)

Staying Current with AML Laws, Regulations and Precedents

There is no simple way to stay current with changes in the Act, its regulations or the current thinking of FINTRAC. However, by paying attention to communications put out by industry associations and other stakeholders including CLHIA, CAILBA , Advocis and IFBC, an advisor can have reasonable assurance that critical changes are not being missed. It is also helpful for the Compliance Officer to subscribe to any available "push" communications from these organizations and regulators. Finally, the Compliance Officer should make a point of visiting the various websites from time to time to make sure that information is not being missed.

Contact Information

FINTRAC - FINTRAC has a "push" communication mailing list, to which you can subscribe from the Home Page. Information regarding insurance can be found at www.fintrac.gc.ca.

CAILBA - Visit www.cailba.com. It is anticipated that the material provided to members will be updated to reflect changes.

CLHIA - Visit www. clhia.ca, The Industry, Material for Financial Advisors for updates.

Advocis - If you are a member of Advocis, visit www.advocis.ca.

IFBC - If you are a member of IFBC, visit www.ifbc.ca.