CAILBA PRODUCER COMPLIANCE GUIDANCE

Appendices

Introduction

This compliance guidance manual has been created by CAILBA for use by Producers associated with CAILBA members. It is proprietary to CAILBA and is copyrighted. It is intended for the exclusive use of the Producer and the Producer's staff. We hope that you will find the material helpful in developing your own compliance program.

It is an understatement to say that the insurance world has changed for all of us. While the regulatory requirements that have been imposed on all of us may be necessary, the task of developing a workable compliance program can seem to be overwhelming. We hope that by providing information and guidance, CAILBA can assist you in accomplishing your compliance objectives.

Before you attempt to develop a compliance program or to fill in the gaps in your existing program, it makes sense to review all of this material carefully. Do a risk assessment. As yourself the following questions:

1. What are the things which, if left undone, could have a really negative effect on my business?
2. What are the regulatory requirements that carry really bad consequences?
3. What are the things that pose reputation risk to me and my business?

It is very likely that you will arrive at the following conclusions:

1. Having the required anti-money laundering program that complies with the Act is vitally important because

- This is a national and international imperative.
- The Government of Canada has made the fight against money laundering and terrorist financing a national priority.
- Money Laundering is prevalent in the insurance business and is not being detected as systematically as it needs to be, according to regulators.
- Failure to maintain an AML compliance regime carries stiff administrative penalties.
- FINTRAC is an activist regulator that is performing audits on Producers.
- Being caught up, even inadvertently, in money laundering and terrorist financing can lead to criminal penalties, severe reputational damage and loss of licence.

2. Having the required privacy program that complies with PIPEDA and provincial privacy laws is extremely important because

- The life insurance business is one of the most information dense businesses, with extraordinary amounts of personal information being exchanged daily.
- Canada is a world leader in privacy legislation and the Office of the Privacy Commissioner is active and empowered to "name names."
- Insurers require appropriate handling of personal information as a contract condition.
- Having a privacy program in place is a requirement under the CAILBA Producer Code of Conduct.
- The reputation risk and financial risk associated with a breach is extreme. The impact of such a breach could have a devastating impact on a Producer's ability to maintain contracts and earn a living.

3. **Understanding and adhering to numerous market conduct laws, regulations, best practices, codes of conduct, traditions and expectations is essential because**

- Producers are regulated provincially and their licences depend on adherence to a number of very specific obligations and prohibitions.
- Provincial regulators are charged with protecting the consumer and they take this role seriously. Their power to issue and revoke licences is a key component of their regulation.
- Insurers have obligations under provincial laws and regulations pertaining to the activities of their Producers and they take these matters seriously. They are obliged to screen, monitor and report Producers. MGAs perform some of these tasks on behalf of insurers. Their own reputations and livelihoods rely on identifying regulatory risks and imposing controls that will mitigate those risks.
- The public and press are very alert and are quick to identify questionable practices.

Review the CAILBA Producer Code of Conduct included in this manual. It contains a listing of numerous market conduct obligations and prohibitions for Producers.

The MGA's Role

MGAs act as intermediaries between life insurers and Producers, providing services to both under contracts. In most provinces, MGAs are regulated as insurance agents. In Quebec and Saskatchewan, they have some additional obligations. At the time of this writing, the Canadian Council of Insurance Regulators ("CCIR") has published a discussion paper on the regulation of MGAs. Of concern is whether there are gaps in regulation that leave the consumer exposed. If it is determined that there are, new regulations are possible. Certainly the emphasis on the MGA's role in maintaining market conduct standards is increasing. The following are some of the obligations that MGAs face. Some are express provisions of their contracts with insurers; others are implied.

1. **Licence and E&O checks**

2. **Screening Producers for suitability to act as Producers**

   The CLHIA created Guideline G8 "Screening Agents for Suitability and Reporting Unsuitable Agents" several years ago and continues to update this material. It was designed with the input of CAILBA and regulators and was intended for use by MGAs in screening Producers. Originally designed in response to Ontario's Duty of Care Regulation, which requires an insurer's board of directors to ensure that their organization screens Producers for suitability, monitors their activities to ensure compliance and reports those Producers who appear to be unsuitable, the Guideline was adopted and applies to all member companies in all provinces.

   The information gathered on the Producer Application for Contract represents the minimum amount of information that insurers believe is necessary to make an informed decision as to whether to accept or reject a candidate or seek more information. The consent on the Application was updated to comply with PIPEDA and provincial privacy laws and to cover the activities that MGAs engage in.

   Screening procedures can include, among other things:

   - Senior management interview to determine suitability and fit within the MGA
   - Filling out of CLHIA Application for Contract
   - Credit check
   - Criminal background check
   - Full retail background report

- A check of CAILBA, IIROC, MFDA and provincial insurance regulators' websites
- Verification of licence and errors and omissions insurance
- Reference checks
- Sign off by senior management on contract
- Review of Producer's
    - methods of holding out
    - standard representations and advertising standards, including websites and the professional use of all social media
    - standard disclosure documents
- Verification and review of Producer's
    - Anti-money laundering program
    - Privacy program and privacy breach procedure
    - Needs-based sales practices
    - Awareness of and adherence to the CRTC Unsolicited Telecommunication Rules, including the National Do Not Call List ("N-DNCL")
    - Records management and file maintenance practices.

3. Monitoring and auditing Producers' activity for compliance with laws and regulations, including:

A. Licensing and errors and omissions insurance checks, including spot checks.

B. Monitoring for Inappropriate Sales Practices including

- Fraud;
- Misappropriation of client funds;
- Forgery;
- Money laundering;
- Selling without a licence or otherwise violating the terms and conditions of a licence;
- Improper use of sales associates and assistants;
- Problems with non face-to-face selling;
- Fronting;
- Breach of privacy or confidentiality laws or rules;
- Violation of holding out laws or rules;
- Failure to disclose a material conflict of interest;
- Tied selling;
- Premium rebating, except to the extent permitted by law;
- Undisclosed replacements;
- Indiscriminate systematic replacements;
- Twisting;
- Churning;
- Poor disclosure, material non-disclosure, including failure to provide the required written disclosures;
- Language barriers and use of unqualified translators;
- Misuse of, or material changes to, company-provided illustrations;
- Incomplete comparisons;
- Poor needs analysis, failure to assess product-client suitability and evidence of KYC problems;
- Inappropriate sales to seniors;
- Inappropriate leveraging;
- Material misrepresentation or omissions;
- Coercion or undue influence;
- Inducements to insure, where prohibited by law;
- Misleading statements to an insurer;
- Incompetence;

- Lack of trustworthiness, where a Producer contract has been terminated for cause;
- Commission-sharing with an unlicensed individual;
- Unnecessary delay in delivering policies or failure to deliver policies;
- Trafficking in insurance policies, where prohibited by law.
- Poor file management and record-keeping;

C. Monitoring Segregated Fund and Other Investment Product Sales including money parked too long in money market funds and market timing.

4. Training Producers, providing and tracking continuing education

5. Providing compliance support to producers ("Value Added Services") often including assistance with needs-based selling tools and disclosures.

6. Complaints management

7. Investigations and reporting unsuitable producers to insurers

8. Responding to insurance company requests for information

9. Responding to regulatory audits and Inquiries and legal proceedings.

CAILBA PRODUCER CODE OF CONDUCT

This Code of Conduct sets out the standards to which we expect our Associate General Agents and brokers (collectively "Producers") to adhere in their dealings with customers and in representing insurers. The Code supplements and reinforces but does not replace industry association, provincial regulatory and insurer codes of conduct to which the Producer may already be subject and forms part of the contract between the Producer and the CAILBA member.

The Principles

The Producer will be diligent and at all times will act with integrity, in the customer's best interests and in accordance with both the letter and the spirit of the laws that apply. The Producer also agrees to adhere to the following Obligations and Prohibitions.

Producer Obligations

Place the Customer's Best Interests First: At all times the Producer will place the customer's best interests before his or her own interests. Recommendations will be for the appropriate amount of coverage, product, strategies and concepts that best meet the customer's circumstances. The Producer will provide service, advice or information only where the Producer is competent to do so, not offering legal or other professional advice outside the scope of his/her knowledge or professional standing.

Hold Out Appropriately: The Producer will not hold out as being a representative of the CAILBA member and will use only marketing materials approved by the member. Any Producer-generated materials (including letters, sales aids, web sites, newspaper and radio ads, seminar presentations or presentations using PowerPoint or similar software) that include the either/or the member's or an insurer's company name or corporate logo must be approved by the member and the insurer. The Producer will:

- Ensure his/her licence is posted in a publicly visible place, where the law requires this.
- Hold out under the name on the licence unless provincial regulation allows otherwise.
- Not mislead as to qualifications or the nature of business being conducted.
- Avoid terms that indicate meaningful specialized training and competency unless the Producer has actually achieved the claimed level of training and/or competency.
- Not claim to have "associates" unless there is at least one licenced individual with equal or better qualifications.
- Not hold out as a financial planner unless holding a planning designation recognized by the Financial Planning Standards Council.
- Ensure that letterhead, business cards and proposals include the name of the sponsoring insurer if the licence is sponsored and one of the following titles:
    - Life Insurance Agent
    - Life Agent
    - Life Insurance Broker
    - Life Broker
    - Life Underwriter
    - Chartered Life Underwriter (if you hold the CLU designation)
    - Financial Security Advisor (Quebec)
    - Financial Planner (Quebec only, with appropriate licence).

Make Needs-Based Recommendations: The Producer will make a diligent and business-like effort to analyze the customer's needs, objectives and financial circumstances in order to determine the appropriateness of the product and/or other recommendations being made. The Producer will base recommendations solely on the established needs of the customer after gathering facts on which to base such recommendations, taking into account the customer's financial position, tolerance for risk and other relevant concerns. Any recommendations will be documented through the use of fact finders, needs analyses or other means and retained in the file.

Make Clear and Accurate Representations: The Producer will

- Make clear, relevant, honest, complete and factual representations.
- Sell products and make other recommendations on their merits.
- Refrain from engaging in defamation of competitors or their products and services.
- Explain accurately and fully the terms and conditions of products, including both guaranteed and non-guaranteed values and features, and the risks and limitations associated with any advice or other recommendations.

Provide Full Disclosure: In accordance with industry guidelines and best practices, the Producer will disclose ***in writing***

- The insurers that the Producer represents.
- The fact that the Producer is an independent broker.
- How the Producer is compensated.
- Whether the Producer is eligible for additional compensation (cash or non-monetary, such as travel incentives) based on factors such as volume of business placed in a specific period of time.
- Any real or potential conflicts of interest. Where avoidance of conflict is not possible and where it is not already prohibited, the Producer will provide disclosure prior to entering into a sale or making a

recommendation.
- The fact that the customer has a right to ask for more information.
- Any fees charged for services in addition to commissions. (A written agreement should be in place in order to charge fees).
- Any commission splits (Quebec).

It is highly advisable for the Producer to sign the disclosure and ask the customer to sign as well, providing one copy to the customer and maintaining one copy in the customer file.

Provide Segregated Fund Point of Sale Disclosures: the Producer will

- Deliver the Information Folder and Fund Facts documents for each segregated fund available under the contract to the customer before he or she signs the application for the IVIC. The customer may choose to receive these disclosure documents either physically (in person, mail, or fax) or electronically (e-mail or viewed by the client on-line).
- Require the customer to sign acknowledging receipt of these documents.
- Ensure that the customer is aware of the rescission right provided by the insurer.

Use Only Approved Sales Illustrations: The Producer will comply with the CLHIA Guidelines (see Reference Material) for Individual Life Insurance Illustrations and use only approved illustration software to illustrate an insurer's products to customers and prospects. It is highly recommended that the Producer submit illustrations that are signed by both the applicant and the Producer with all applications that are submitted. Universal Life illustrations that match the sale that was made, including the details contained in the application, are required.

Avoid Conflicts of Interest: A conflict exists when a reasonable person would suspect or believe that an activity or relationship places the Producer's interests in conflict with the interests of the customer. See "Exercising Discretionary Authority" below. Wherever possible, the Producer will avoid all real and perceived conflicts of interest.

Recommend Replacements Only When it is Appropriate to Do So: While it is not by itself evidence of unsuitable conduct, a replacement should only be undertaken when it is in the customer's best interests. The Producer must be able to demonstrate the appropriateness of any replacement.

The Producer is expected to be familiar with and adhere fully to the provincial regulations that apply, regardless of whether the replacement is internal or external.

Recommend Leveraging Only When it is Appropriate to Do So: Prior to recommending a leveraged transaction, the Producer will determine that leveraging is appropriate for the customer, given risk tolerances and personal circumstances. This requires the Producer to ensure that the customer:

- Understands and accepts the increased risks and servicing requirements of leveraged investing.
- Has received all required disclosure and point of sale documents including an illustration where required.
- Has a long-term investment objective or intends to speculate and understands the associated risks.
- Has the capacity to sustain losses and repay the remaining loan balances if the plan needs to be unwound and understands their obligations under the loan.
- Has appropriate investment knowledge based on the type of leverage applied for and the

customer’s existing investment portfolio.
- Can tolerate the added risk of leveraged investing.
- Has the financial capability to service loan interest, taxes and principle repayments without drawing on the leveraged program or selling other long term investments or assets.

Obey the Rules for Referrals and Referral Fees: Referral arrangements consist of a flat fee paid for each lead or prospect, *regardless of whether a sale eventually occurs*. These payments cannot be contingent upon a sale and cannot be a percentage of the commission earned unless the payment is being made to another licenced individual. The Producer will disclose details of referral arrangements to customers.

Obey the Rules for Commission Splitting: Commission splitting consists of the payment of a fee or an exchange of something of value that is based on a percentage of commission earned on a sale and/or is contingent on the sale of a life insurance product. Before splitting commissions with another Producer, the Producer will ensure that person is appropriately licenced where necessary in order to receive the split. The Producer will disclose details of commission splitting to customers.

Protect Privacy & Confidentiality: The Producer has a duty to protect the confidentiality of information provided and the privacy of those who provide it. **As required by PIPEDA, the Producer will establish a Compliance Program that includes:**

- Naming a Compliance Officer
- Written Privacy Policies and Procedures including
    - Receiving and Processing Access Requests
    - Receiving and Responding to Inquiries and Complaints
    - Safeguarding Information
    - Privacy Breach Procedures
- Procedures for regular assessment of the privacy Program
- Ongoing training of Producer and staff

The Producer will:

- Use only lawful means to collect personal information.
- Inform the customer what information must be disclosed in order to conduct business on the customer's behalf.
- Obtain confidential information regarding a customer's personal or business affairs only directly from, or with the permission of the customer.
- Obtain written consent from the customer to collect personal information, which includes notice of information sharing with the MGA. The Producer will not rely exclusively on the consents that insurers obtain on their applications.
- Not disclose information concerning the customer to any third party without the customer's written authority to do so.
- Disclose information when it is required by order of lawful authority.
- Protect all personal information about a customer with appropriate security safeguards.
- Not make photocopies of the medical information on applications or medical reports required by life insurance companies in the normal course of business; not retain any such information beyond the date of contract issuance.

Respect Copyrights: The Producer will respect copyrights and obtain permission to post material written by someone else in his communications and on his or her website. This includes articles, strategies, news articles theories and other information, use of any company's logo or information about its products. If the Producer chooses to link to other sites, the link should be to that site's home page, ensuring that the owner's contact information is provided.

Deliver All Documents Immediately: The Producer will not hold or retain customer documents. Documents will be delivered to the customer within a reasonable timeframe and any required delivery receipts will be obtained.

Handle and Report Complaints Appropriately: The Producer will

- Comply with Quebec's requirements for complaint management, if doing business in Quebec.
- Attempt to resolve service related complaints.

Maintain a Complaint Log: The Producer will maintain a complaint log to track complaints, to provide any required reports and to maintain a state of readiness for regulatory and other audits. The complaint log should maintain information in a consistent fashion. At a minimum, it should summarize the following:

- Customer name
- Policy or document number
- Producer name
- Date of complaint, (written or verbal)
- Recipient of complaint
- Individual handling the complaint
- Summary of complaint (details should include whether a regulatory body is involved.)
- Whether the complaint was reported to the insurer and/or MGA and the contact information.
- Steps towards resolution
- Statement of resolution and date of resolution.

Create and Maintain an Anti-Money Laundering Program: As required by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the "Act"), the Producer will adopt a compliance regime and ensure that the Producer, employees and those who *act on behalf of the Producer* comply with the Act. The Act requires:

- Assessing and documenting the money laundering and terrorist financing risks unique to the Producer's business.

- Appointing a Compliance Officer.

- Developing detailed, auditable compliance policies and procedures for reporting and record-keeping.

- Ongoing review of the effectiveness of the compliance program through self-assessments and/or audits.

- Compliance training and a forward-looking training plan for employees, agents or others acting on the Producer's behalf.

Comply with CRTC's Unsolicited Telecommunications Rules, including National Do Not Call List "N-DNCL." The Producer and any person or entity that telemarkets on behalf of the Producer will:

- not attempt to telemarket to numbers that are on the N-DNCL without express prior consent.
- register with the N-DNCL Operator, who registers consumers' numbers for the list and pay any required fees.
- comply fully with the rules on referrals, established business relationships and service calls.

Keep Accurate and Substantial Books & Records: The Producer will

- maintain enough information in customer files to be able to demonstrate the appropriateness of any advice given or sale made and will retain all material information used in the negotiation, maintenance or servicing of a policy or contract.
- Make any and all requested books and records available to the MGA and/or insurer upon request.

Maintain active licences and the required errors and omissions insurance: The Producer will

- Maintain uninterrupted licence and E&O in any province in which the Producer sells insurance or provides service to customers.
- Arrange and pay for extended errors and omissions coverage if leaving the business, retiring or selling the practice.

Notify the MGA immediately of :

- Any license or E&O lapses, cancellations or other changes.
- Any privacy breaches or complaints.
- Any market conduct related complaints.

- If you are or have been
    - charged with or convicted of any crimes
    - the subject of a regulatory investigation
    - subject to garnishments or have or will enter into bankruptcy or insolvency.
    - In a conflict of interest situation
    - In receipt of a consumer complaint that you cannot easily resolve
    - the recipient of a complaint about privacy

Producer Prohibitions

Exercise of Discretionary Authority: The Producer must act on explicit customer instructions only and will retain proof of the date and details of this instruction in the customer's files. The Producer is prohibited from exercising discretionary authority over customer accounts and from entering into any of the following relationships unless the customer is a close family member *and* the relationship is disclosed and approved in writing by insurers who require approval:

- General Powers of Attorney over the customer's financial affairs.
- Trusteeships where the Producer exercises control of the trust's assets.
- Executorships over a customer's estate; Borrowing money from or lending money to customers.
- Being named as beneficiary of a policy sold or serviced by the Producer.

Discretionary authority includes letters of direction, pre-signed blank or partially blank forms, formal powers of attorney, trusteeships, account signing authority, executorships or any similar legal instrument.

Fronting: The Producer will not submit an application on behalf of an unlicenced person or a person who is not authorized to represent the insurer whose application is taken. Where more than one Producer has been involved in a sale, all Producer names and codes will be recorded on the application.

Rebating and Inducements: The Producer will not offer or provide rebates or inducements to insure where this is prohibited by law. This includes waiving fees or returning a fee if a sale is completed. Where rebating is not prohibited by law, any agreement a Producer makes to rebate premium to a customer is an agreement between the Producer and customer and does not involve the CAILBA member or insurer. Such agreements will be in writing at time of sale and will disclose that the insurer and the CAILBA member are not parties to the rebate.

Viatical Agreements/Life Settlements/Stranger Owned or Investor Owned Life Insurance: Financial vehicles involving the direct or indirect purchase of the death benefits of life insurance policies through the payment of a discounted price for the policy benefits while the Insured is still alive is prohibited. Acquiring ownership of life insurance contracts or a financial interest in life insurance contracts for investment purposes where there is no insurable interest is prohibited.

Payments: Neither the CAILBA member nor insurers will accept the following forms of payment from Producer or customers. The Producer will not

- Remit, on behalf of customers, payment for premiums or other transactions using a personal cheque or a cheque issued by the Producer's company.
- Accept cheques or money orders from customers made payable to "cash" or to the Producer. All cheques or money orders will be made payable to the life insurance company.
- Accept cash for the payment of premiums.

Twisting: The Producer will not engage in "twisting" which is the unethical act of persuading a policyholder to drop a policy solely for the purpose of selling another policy, without regard to possible disadvantages to the policyholder.

Churning: The Producer will not churn customer accounts by making excessive or unnecessary changes to insurance or investment contracts that result in generating commissions but have no discernible benefit to the customer. If the Producer acts for customers on transactions permitted under the terms of a Limited Power of Attorney (LPOA), the Producer may only act after discussing and securing the agreement of the customer. The only acceptable LPOA for this purpose is one approved for use by the life insurance company.

Tied Selling: It is an offence to make the purchase of one product conditional upon the purchase of another product. The Producer will not engage in tied selling or impose other conditions on any customer.

Forgery and Alteration of Documents: According to the Criminal Code of Canada: *366. (1) Everyone commits forgery who makes a false document, knowing it to be false, with intent (a) That it should in any way be used or acted on as genuine, to the prejudice of any one whether within Canada or not; or (b) That a person should be induced, by the belief that it is genuine, to do or to refrain from doing anything, whether within Canada or not. Making false document (2) Making a false document includes (a) Altering a genuine document in any material part; (b) Making a material addition to a genuine document or adding to it a false date, attestation, seal or other thing that is material; or (c) Making a material alteration in a genuine document by erasure, obliteration, removal or in any other way.*

Forgery is fraud, which is a criminal act that must be reported to the appropriate authorities. All costs associated with remediation of contracts or settlements will be charged to the Producer. Examples of forgery and fraud include:

- Signing a customer's signature or that of another Producer, or initialing a change with the intention that the insurer will act on either as if they were genuine. A Producer may not sign the customer's name or the name of anyone party to the contract to a document even if the customer authorizes it. All signatures must be authentic.
- Obtaining pre-signed blank forms.
- Signing as a witness to a signature that has not actually been witnessed.
- Signing as witness to a signature that is known to be forged.

Engaging in criminal behaviour while performing the duties of an agent.

Selling insurance or providing advice without having a valid insurance licence and/or errors and omissions insurance.

Use of Sales Associates and Assistants: The Producer will not allow unlicenced sales associates and/or assistants to perform any activity for which a licence is required.

GUIDANCE ON CREATING ANTI-MONEY LAUNDERING AND ANTI-TERRORISM FINANCING COMPLIANCE PROGRAM FOR PRODUCERS CONTRACTED WITH CAILBA MEMBERS

Note: Information provided in bold italics represents guidance or best practices which should prompt you to decide on a process. Once you have done so, the bold and italicized material is to be deleted, rewritten as a process or maintained as background information. Information provided in normal font ***is suggested language or process for your compliance regime.***

References to "us", "our" and "we" are in fact references to the Producer. If you are a sole proprietor, you may wish to use first person voice in this document by referring to "I", "my" and "mine". It is expected that anyone wishing to adopt the compliance program will have to edit the document to accurately reflect their unique situations.

Once completed, this document may serve as your AML compliance manual. Note, however, that it is crucial for you to actually perform the activities described herein. If you cannot do so, you should consider amending the document to better identify how you comply with the requirements. It is inadvisable to adopt policies and procedures that you do not follow.

The face page of this document is designed to allow you to carry out scheduled activities without having to make changes to the document itself.

Effective Date:

Revised on:

Risk Assessment Date:

Self-Assessments/Reviews:

Appointed Compliance Officer(s):

Signature of Senior Officer: ____

Date: ____

This manual incorporates elements of 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, which was intended for use by insurers' distribution partners.

TABLE OF CONTENTS

What the Act Requires Producers to Do

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the "Act") applies to life insurance brokers and agents, who are defined as "an individual or entity licenced provincially to carry on the business of arranging contracts of life insurance." While MGAs are not named specifically, it appears that the Act applies to MGAs as well because they are involved in "arranging contracts of life insurance." Independent brokers and insurers are both directly subject to the provisions of the Act, which requires insurance agents and brokers to adopt a compliance regime and ensure that their employees and those who *act on their behalf* comply with the Act. While selling an insurer's products, a broker is generally deemed to be that insurer's representative or agent.

Note: Independent brokers and AGAs who hold contracts with MGAs do not act on behalf of the MGA. Collectively, brokers and AGAs are known as "Producers" unless specifically referred to otherwise.

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. Appointing a Compliance Officer.
2. Assessing and documenting the money laundering and terrorist financing risks unique to our business.
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 our behalf as well as 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 a Producer 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 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. "

Guidance: This Guidance is designed to assist you in complying with the Act. The Compliance Officer is the most important person within the Compliance Regime. This material is written with the view that the Producer is the Compliance Officer. It this is not the case, you must amend the language accordingly. While you are required to train your staff on numerous AML topics, do not expect them to become experts. It is important for them to understand what a STATR is, for example (see below), but do not expect them to know how to file one. That is the Compliance Officer's (Producer's) job. Much of the information provided below is provided for the benefit of the Producer. Staff must receive regular refresher training, which includes much of this material, but their main focus should be on ensuring they understand the reasons behind the questions on the checklists provided and that they are alert to things that make no sense or seem out of place in their day-to-day activities.

Appointment of Compliance Officer(s)

Under the Act, Compliance Officers are responsible for:

- Implementing and monitoring the compliance program;
- Establishing and revising policies and procedures and risk assessment as required;
- Initial and continuing training of any representatives, employees and persons acting for and on our behalf;
- Making any necessary and required declarations and/or reports to authorities;
- Immediately notifying the Producer (if the Producer is not the Compliance Officer) and any other principals of any known or presumed violation of our compliance program.

Under existing rules, we may obtain the assistance of another person to manage our 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.

(According to FINTRAC, the Compliance Officer needs the "authority and resources necessary to discharge his or her responsibilities effectively." The CLHIA suggests that the Compliance Officer should be someone senior, in a decision-making role, with the ability to effectively promote AML activities. This person must be in a position to intervene when situations arise and able to ensure that you comply with the Act. The Compliance Officer must be able to demonstrate knowledge of the organization's AML policies and responsibilities and to conduct investigations as well as train staff and maintain the information required. This document assumes that the Producer is the Compliance Officer.

Risk Assessment

(A risk matrix template that you can customize, along with explanatory notes, are attached as Appendices A1 and A2. FINTRAC's Guideline 4, Appendix 3, "Risk Level Assessment Matrix" is Appendix A3. It provides useful guidance on how to assess risk. All three appendices are intended to be read together).

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. It should focus on any unique risks we have identified for our business including product risk, customer risk, geographic risk and other risks.

Compliance Procedures (Risk Management and Mitigation)

Guidance: Identify any unique or complicated features of your business model and amend the language of this section accordingly. Consider whether you outsource back room activities, specialize in niche markets, do a material percentage of your business in known high crime areas, have complicated distribution arrangements or any other features that would not be considered typical of a Producer).

According to FINTRAC, "Risk mitigation is about implementing controls to limit the potential money laundering and terrorist financing risks you have identified while conducting your risk assessment to stay within your risk tolerance level. As part of your compliance program, when your risk assessment determines that risk is high for money laundering or terrorist financing, you have to develop written risk-mitigation strategies (policies and procedures designed to mitigate high risks) and apply them for high risks situations".

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 *customers* who are intent on exploiting these products' advantages also pose risks. Insurers face these risks directly. We rely on their controls in addition to those we must implement 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.

Special Measures for High Risks

According to FINTRAC, "You have to take reasonable measures to conduct ongoing monitoring of financial transactions that pose high risks of money laundering and terrorist financing to detect suspicious transactions. Reasonable measures may involve manual or automated processes, or a combination of both depending on your resources and needs. They also depend on the size of your business and the risks to which you are exposed. You do not necessarily have to create or purchase an electronic system. You can use your available resources and business processes and build on these. Your policies and procedures have to determine what kind of monitoring is done for particular high risk situations, including how to detect suspicious transactions. Your policies and procedures should also describe when monitoring is done (its frequency), how it is reviewed, and how it will be consistently applied".

Best Practices:

- ***Identify customers who have applied for or own high risk non-registered products. Assess these customers as high, medium or low risk based on the information available to you about their businesses, travel, behaviours, etc.***
- ***Review all applications for non-registered high risk products with deposit amount of $10,000 or more for red flags before submitting.***
- ***Discuss any concerns with your MGA's and insurer's AML contacts.***

You could consider the following measures to monitor high risk situations:

- ***Flag activities or changes in activities from your expectations and elevate concerns as necessary;***
- ***Set business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review.***

Insert a description of any procedures you intend to follow here.

Proposed procedure:

- ***Flag all cases involving PEFPs or any other high risk customers that are identified by use of the checklist***
- ***Monitor closely, reviewing all transactions.***

Insert your procedure here.

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.

Form of Reports – Refer to FINTRAC Guideline 8. If we have the necessary electronic technical capabilities to file electronically, we must do so wherever it is FINTRAC's preferred method.

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 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. We are prohibited from disclosing to the customer that we have filed a report. In fact, while it is acceptable to discuss our concerns with the MGA or insurer, the decision as to whether to file a STATR is ours alone and should not be divulged to either party. 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. ***Guidance: You must apply to FINTRAC for a code to make electronic reports.***

According to FINTRAC, "there are penalties if you fail to meet the suspicious transaction reporting obligations. Failure to report a suspicious transaction could lead to up to five years imprisonment, a fine of up to $2,000,000, or both. Alternatively, failure to meet the suspicious transaction reporting obligations can lead to an administrative monetary penalty. There are also penalties if you tip anyone off about a suspicious transaction report, if your intent is to harm or impair a criminal investigation. For more information on penalties, you can also consult the Penalties for non-compliance section of FINTRAC's Web site. Penalties for failure to report do not apply to employees who report suspicious transactions to their superior."

Guidance: If at all possible, flag high risk customers and policies that have given rise to a STATR or other reports on your computers. Any changes in parties to a policy or the policy itself should trigger a review by the Compliance Officer.

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 should immediately review **FINTRAC Guidelines 3A and 5** to determine *whether* to report and *what* to report. As of the date that the Compliance Officer determines that reasonable grounds exist, you have 30 days to make any report.
3. Where a STATR has been filed, monitor policy level and customer level activity on any affected policies for which you have records.
4. Flag policy/associated policy/customer 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.

LCTR Procedure:

Neither MGAs nor insurers 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 have to 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/ for monitoring and reports or set up a manual process for monitoring.
4. The Compliance Officer may consult with the affected MGA and insurer regarding the case, but should not discuss any decision about filing a STATR.

Terrorist Group or Listed Property Report Rules:

We are a "reporting entity" with a legal obligation to send a terrorist property report to FINTRAC if you have property in your possession or control, including premium payments and insurance policies, that you (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 you or any of your “associated persons” (defined here as employee staff members) encounters any such circumstance, you may not complete or be involved in the transaction or attempted transaction. You must remove yourself 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. **See FINTRAC Guideline 5, section 3.2 for CSIS and RCMP contact information and Guideline 8.3 for information on obtaining forms.**

Terrorist Group or Listed Property Report Procedure:

1. When an attempted or completed transaction is escalated by a staff member or is detected by the Compliance Officer, the Compliance Officer should immediately review **FINTRAC Guideline 7**, 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) ***is not processed.*** Under the Criminal Code, it may have to be frozen.
5. **Compliance Officer may flag the policy/associated policies/customer and freeze activities or set up a manual process for monitoring.**
6. The Compliance Officer should check with the MGA and insurers as to their requirements for notification of this kind of report.

Written Records Required for Selling Producers and Insurers

(See FINTRAC Guideline 6, Section 3.1 for general exceptions to record keeping, which include exempt policies, registered products and products that exist for protection only and not for investment purposes. While it is helpful to know the exemptions, practically speaking, Producers consistently capture the information required because insurers embed sections on their applications and forms. It is important for you to assess exactly how you capture this information and to identify any gaps in record-keeping that require repair).

Large Cash Transaction (“LCT”) Record Rule:

Insurers and Producers 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:

Insurance carriers have a "no cash" policy, which means the likelihood of having to maintain this record is virtually nil.

1. If an attempt was made to pay by cash and this is suspicious, we must file a STATR with FINTRAC.
2. If cash was actually received, we must file an LCTR.
3. Maintain any actual LCT record.
4. Flag policy/associated policies/customer for monitoring and reporting.

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, Producers must 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:

Insurance companies have embedded client ID requirements in their applications and supporting material, where necessary. ***(Guidance: The Producer must review all such applications and supporting material to verify this statement or determine how to amend it).***

1. Review applications/forms for good order.
2. Retain copies of Client ID information.
3. Flag policy/associated policies/ customer for monitoring and report.

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. We must maintain the record.

- If the entity is a corporation:
  - the name and occupation of all directors of the corporation; and
  - the name, address and occupation of all individuals who directly or indirectly own or control 25% or more of the shares of the corporation.
- If the entity is other than a corporation:
  - the name, address and occupation of all individuals who directly or indirectly own or control 25% or more of the entity.

Where this requirement is not part of the Insurance Company Third Party forms, the agent should request the information from the customer and provide in written form to the MGA..

Beneficial Owners Record Procedure:

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

1. Where allowed, keep copies of non-medical applications for administrative purposes to capture initial ID. Where not allowed, transfer the required information to a permanent record.
2. If an insurer notifies us that it has identified high risk customers who trigger the requirement to update, notify the MGA.
3. Where we become aware of a high risk customer, monitor their policies and transactions going forward.
4. Flag policy/associated policies/ customer for monitoring and reporting.

See FINTRAC Guideline 6 for more information about the requirements.

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 our client identity verification.

1. Verify that the application is in good order before passing it through to the MGA or insurer.
2. Retain a copy of the record.
3. Flag policy/associated policies/ customer for monitoring and reports.

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. Retain copies of the record.
2. Compliance Officer may flag policy/associated policies/customer for monitoring and reports or set up a manual process for monitoring.

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

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. If $100,000 or more has been received in a single payment, ask the customer whether he or she is a PEFP.
2. Retain copies of the record.
3. Flag policy/policies/customer for monitoring and reports.

Records Retention Requirements:

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.

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 you 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 the Producer 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 an action plan and timeline for implementation.

Failure to deliver the report within thirty days of a review could lead to an Administrative Monetary Penalty of up to $100,000. **See Appendices B1 and B2 for a copy of a checklist and template for a report.**

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." ***Guidance: FINTRAC has explained that the training program must be in writing and be maintained. The written program should lay out the frequency and methods of training (formal, on-the-job or external). New staff should be trained immediately after hiring. The method of training may vary greatly depending on the size and complexity of the business. At a minimum, training should cover the background about money laundering that is relevant to our business, actual regulatory requirements and penalties as well as the policies and procedures we have put in place to deter and detect money laundering. FINTRAC has expressed the expectation that all who receive training should understand how it relates to the jobs they perform.***

Staff must be educated as to how Producers and the industry are vulnerable to abuse by criminals laundering the proceeds of crime or by terrorists financing their activities. Examples of how Producers and MGAs can be used to launder illicit funds or fund terrorist activity should be included. Finally, employees 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.

See Appendix C for a copy of PowerPoint training. Additional training is often made available on an ad hoc basis and can consist of training developed 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 by MGAs are also made available. Records of attendance at training should be 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, paying attention to communications put out by industry associations and other stakeholders including CLHIA, CAILBA , Advocis and IFBC, provides 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, 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.

CLHIA - Visit www. clhia.ca. Click on 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.

GUIDANCE - PRIVACY PROGRAM REQUIRED BY PIPEDA

Introduction

The Personal Information Protection and Electronic Documents Act ("PIPEDA") applies to all organizations, including Insurance Producers, engaged in commercial activities across Canada, except in those provinces that have substantially similar laws. PIPEDA also applies to the *federally-regulated* private sector regardless of where situated and to personal information ("PI") in inter-provincial and international transactions. Because virtually all insurers with which insurance Producers do business are federally regulated, the *customer* information you collect, use and retain on behalf of insurers or on behalf of your customer is subject to PIPEDA. The information MGAs collect on Producers as part of their screening and monitoring is protected by PIPEDA or by substantially similar provincial regulation.

PIPEDA applies to *employee* information *only* in organizations that are engaged in federal works, undertakings or businesses, such as most insurers. Because Producers are provincially licenced and regulated, provincial laws govern personal information you might collect on employees. This makes the terrain a bit more complicated if there are local disputes or complaints that would require you to navigate through different processes for resolution. However, as a best practice, in the interests of fairness and in order to ensure that you are compliant with provincial laws, we suggest that you protect your employees' information consistent with the way that you protect customer information.

Guidance: This manual will not provide detail on employee PI management. It is highly advisable to adopt a process that is consistent for employees and customers. It is also recommended that you use clear consent forms consistent with PIPEDA's principles when considering an individual for employment and collecting PI. However, it is up to the Producer and his or her legal counsel to determine the extent to which you are required by provincial law or willing to apply PIPEDA policies to such things as employee access to information, granting of consent and withdrawal of consent.

See "Contact Information" at the back of this manual for information regarding federal and provincial contacts.

A Summary of PIPEDA

You must obtain an individual's consent when you collect, use or disclose the individual's personal information ("PI"). An individual has a right to access PI you hold on them and to challenge its accuracy. PI can only be used for the purposes for which it was collected. If you wish to use it for another purpose, you must obtain consent again. You also need to assure individuals that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption.

Complaints: An individual may complain to you or the OPCC about any alleged breaches of the law. The OPCC may also initiate a complaint, if there are reasonable grounds.

Application to the Federal Court: After receiving the OPCC's investigation report, a complainant may apply to the Federal Court for a hearing under certain conditions set out in the Act. The OPCC may also apply to the Court, which can order you to change your practices and/or award damages to a complainant, including damages for humiliation suffered.

Audits: With reasonable grounds the OPCC may audit your PI management practices.

Offences: It is an offence to:

- destroy PI that an individual has requested;
- retaliate against a covered employee who has complained to the OPCC or who refuses to contravene Sections 5 to 10 of the Act; or
- obstruct a complaint investigation or an audit by the OPCC.

Definition of PI:

PI includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- age, name, ID numbers, income, ethnic origin, DNA or blood type;
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).

Provincial Privacy Laws – Variations:

Currently Alberta, Quebec and British Columbia have substantially similar privacy laws. Ontario has enacted a law that is substantially similar in its treatment of personal health information. The OPCC, Alberta and British Columbia have signed a memorandum of understanding, in an effort to collaborate and cooperate in their approaches to regulation.

Generally, provincial acts are distinguished from PIPEDA not by their *content* but rather by the manner in which they *are or can be enforced*. The provinces have been granted greater "coercive powers" and provincial acts appear to have more teeth. The Commissioner in Alberta, Quebec and BC can make binding orders. In Alberta and Quebec, these orders can be made into binding orders of the provincial courts and organizations can face significant fines for violating the Act. In all three provinces, the Commissioner can "name names," (although BC has not shown a preference for doing so). Employee information also enjoys protection in all 3 provinces. Overall, however, the provinces approach privacy protection in a similar manner to the OPCC, seeking to resolve disputes directly and then through mediation.

Alberta's law, known as "PIPA" is virtually identical to PIPEDA and is complaint-driven like PIPEDA. The Alberta Privacy Commissioner has more latitude than is allowed for under the federal act but Alberta tries to resolve disputes through fact-findings, mediation and education.

The **BC** Act (also known as "PIPA) differs from the Alberta Act with respect to enforcement powers. The BC Privacy Commissioner has express audit powers, but the orders of the BC Commission do not become orders of the Court, as they can in Alberta and Quebec.

The **Quebec** Act, known as "An Act Respecting the Protection of Personal Information in the Private Sector," reflects the fact that privacy is a right guaranteed by Quebec's Charter of Rights and Freedoms. Damages can be sought in the courts and violations of the Act are punishable by significant fines. However, like Alberta and BC, Quebec attempts to mediate disputes first.

Ontario's Personal Health Information Protection Act is substantially similar to PIPEDA in its treatment of health information. PIPEDA applies in all other respects in Ontario. Protection of employee information, other than in federally-regulated endeavors, represents a gap.

Also note that some provinces have rules relating to personal information that is sent outside of province. You should become familiar with the privacy laws in the provinces in which you operate.

Insurers' and MGAs' Contractual Requirements

IMPORTANT NOTE:

You gather, use and retain information about your customers for submission to insurers in order to determine their needs and identify suitable products and recommendations. You do this on your own behalf. When you pass some or all of this information through to the insurer on an insurance application, you generally do this on behalf of the insurer pursuant to a written contract. However, not all insurers include MGAs in their consents in their applications and forms. Because you likely collect more information than you submit on an application, you must ensure that you have the customer's explicit written consent to collect, use and retain the information. Furthermore, because you may use MGA services that are not explicitly covered by the consents insurers attach to their applications (e.g. general marketing support), you must ensure that the written consent you receive from the customer includes consent to share PI with us.

PIPEDA's 10 Principles – Your Responsibilities and How You Can Comply

PIPEDA incorporates the 10 principles of Canadian Standards Association's *Model Code for the Protection of Personal Information* and imposes certain responsibilities on MGAs and Producers regarding how they handle customers' personal information in their possession. Our Privacy Policy is designed for Producers, so that you understand how we manage your personal information as well as that of your customers. ***Guidance: You must have your own privacy policy, which speaks to PIPEDA's requirements. It should be posted on your website and available in print form and electronic form for your customers. See Appendix D, CAILBA Privacy Policy for an example.***

Principle 1 - Accountability:

Requirement:

- Appoint an individual to be responsible for your compliance.

How You Can Comply: See "Appointed Compliance Officer" below.

Requirement:

- Protect all PI you hold or transfer to any 3rd party for processing.

How You Can Comply: ***Guidance: CAILBA members are expected to adhere to the Privacy Policy and to have standards that are consistent with insurers'. You have a right to inquire about our privacy safeguards for information. Once again, it is imperative that you ensure that the MGAs through which you place your business are mentioned in the consents you receive from customers.***

Requirement:

- Develop and implement PI policies and practices.

How You Can Comply: See draft Privacy Policy (Appendix D), which you can amend to fit your practices. Also see information on developing a Compliance Program below.

Principle 2 - Identify Purposes for Collection:

Requirements:

- Before or when you collect any PI from an individual, identify why it is needed and inform the individual from whom it is collected why and how it will be used.
- Document why the PI is collected.
- Identify any new purpose for the PI and obtain the individual's consent before using it.

How You Can Comply: See the draft Privacy Policy, which you can amend to suit your business practices. If you want to use PI for a new purpose, for which you have not received consent, you must obtain consent prior to use.

Principle 3 - Consent:

Requirements:

- Provide clear explanation of the purposes for the collection, use or disclosure of PI.
- Obtain the individual's consent before or at the time of collection, and when a new use is identified.

How You Can Comply: See draft Privacy Policy and Principle 2 above.

Principle 4 - Limit Collection of Information:

Requirements:

- Do not collect PI indiscriminately.
- Do not mislead people about the reasons for collecting PI.

How You Can Comply: See draft Privacy Policy. Collect only that customer information required to issue a policy or to create a file that allows you to demonstrate the appropriateness of the sale.

Principle 5 - Limit Use, Disclosure, Retention:

Requirements

- Use or disclose PI only for the purpose for which it was collected, unless the individual consents, or the Act authorizes use or disclosure.
- Hold onto PI only as long as it is needed to satisfy the stated purposes.
- Implement procedures for retaining and destroying PI.
- Keep PI used to make a decision about an individual for a reasonable time period so that the person can get information after the decision and seek redress.

- Destroy information that is no longer required for a stated purpose or legally required.

How You Can Comply: You collect, use and retain a significant amount of PI from individuals in order to perform the functions you identify in your Privacy Policy.

Principle 6 - Accuracy:

Requirement: Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to 3rd parties.

How You Can Comply: Make every effort to ensure that the information provided to insurers is complete and accurate.

Principle 7 - Safeguards:

Requirements:
- Protect PI against loss or theft.
- Safeguard PI from unauthorized access, disclosure, copying, use or modification.
- Protect PI regardless of the format in which it is held.

How You Can Comply: See "Safeguarding information" below.

Principle 8 - Openness:

Requirements:
- Inform individuals that you have policies and practices for managing PI.
- Make these policies and practices understandable and easily available.

How You Can Comply: See draft Privacy Policy, which you can amend, post on your website and provide on request.

Principle 9 - Individual Access:

Requirements:
- When requested, inform individuals if you have any PI about them.
- Explain how it is/has been used and provide a list of any organizations to which it has been disclosed.
- Give them access to their PI.
- Correct or amend any PI if its accuracy and completeness is challenged and found to be deficient.
- Provide a copy of the PI requested, or reasons for not providing access, subject to exceptions set out in Section 9 of the Act.
- Note any disagreement on the file and advise 3rd parties where appropriate.

How You Can Comply: See "Receiving and processing access requests" below.

Principle 10 - Provide Recourse:

Requirements:
- Develop simple and easily accessible complaint procedures.

- Inform complainants of their avenues of recourse. These include our MGA's own complaint procedures, those of industry associations, regulatory bodies and the Office of the Privacy Commissioner of Canada.
- Investigate all complaints received.
- Take appropriate measures to correct information handling practices and policies.

How You Can Comply: See “Receiving and responding to inquiries and complaints” below.

The Compliance Program

Guidance: In addition to adhering to the 10 Principles of PIPEDA described above, you are required to have a specific privacy compliance program in place. The required elements of the program are consistent with the compliance regime requirements under The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the “Act”).

Appointed Compliance Officer

The OPCC indicates that the Privacy Compliance Officer (“PC Officer”) needs the authority to intervene on privacy issues relating to any of your work. In particular, this person must have the ability to respond to investigators, auditors and the OPCC. Identify your PC Officer and contact information on the face page of your compliance manual, in your Privacy Policy and on your website. In most cases, the Producer will be the Compliance Officer.

Privacy Policies and Procedures

Receiving and processing access requests - the Rules

It is expected that access requests will be relatively rare.

Any customer information you obtain that is required by the insurer for issuance of a policy is collected under the insurer’s consent. Any additional information that you obtain, which is not passed through to the insurer, must be collected under a consent that you obtain directly from the customer. This includes needs analyses and any other information that relates to your relationship as an advisor or financial planner with the customer. When you receive an access request from a customer, you must determine whether the information requested was collected on behalf of the insurer or for your own practice. If a customer wishes to access the needs analysis only, the Producer will have to respond to the request. Realistically, any access request will be more general and will involve information collected on behalf of both insurer and Producer. In contacting both MGA and insurer, from time to time you or the MGA may be asked to respond. Either way, written instructions from both parties is advisable.

The following rules apply:

1. The response to a customer’s access request must be made within 30 days. This can be extended for a maximum of 30 additional days, if:
    - responding to the request within the original 30 days would unreasonably interfere with the parties’ activities
    - more time is necessary to conduct consultations or to convert PI to an alternate format.
2. If a time extension is needed, the individual must be notified within 30 days of receiving the request, and of his or her right to complain to the OPCC.
3. Assistance must be provided to any customer who needs to prepare a PI request.

4. The individual may be asked to supply enough information to enable the parties to account for the existence, use and disclosure of PI.
5. Access must be provided at minimal or no cost to the individual.
6. The individual must be notified of the approximate costs before processing the request and asked to confirm that the individual still wants to proceed with the request.
7. The requested information must be understandable and acronyms, abbreviations and codes must be explained.
8. The parties must send any information that has been amended, where appropriate, to any 3rd parties that have access to the information. This includes MGAs.
9. The individual must be informed in writing when an access request is refused, setting out the reasons and any recourse available.

Customer Access Requests – *Suggested Procedures* - If you receive a request directly from a customer:

1. Be careful not to help the customer "crystallize" a complaint. Ask questions, but don't attempt to write their concerns for them.
2. Anyone, including the Producer, making a request on someone else's behalf needs written authorization from the owner of the PI.
3. Notify the MGA's PC Officer of the request, who will likely notify the insurer(s)' contact person directly and ask for written instructions as to whether they will handle the request or require the MGA to be involved. The MGA will require instructions on handling any PI in our possession, including whether the information needs to be provided in a certain format, the deadlines for providing the information, etc.

Producer Access Requests: Make any access requests for your own PI directly to the MGA's PC Officer.

Receiving and Responding to Inquiries and Customer Complaints – Suggested procedures:

If you receive a privacy-related complaint directly from a customer:

1. Get the facts and attempt to resolve the complaint immediately, if that is possible. At the same time, be careful not to assist in forming the complaint, as this often "crystallizes" a complaint in a manner that the individual never intended.
2. Notify the MGA's PC Officer immediately, who may:
    - notify the insurer(s) involved and ask for written instructions if the MGA's assistance is required in providing PI or resolving the complaint;
    - ask to be kept apprised so that you any necessary changes to policies and procedures can be made and the complaint can be closed off in our complaint log.

Producer inquiries or complaints: Notify the MGA's PC Officer.

Safeguarding information

How you safeguard PI is very likely the most critical element of your privacy efforts, given the sensitive nature of information that you collect directly and indirectly, which you use and retain.

You must have appropriate safeguards to ensure that PI is protected from loss, theft and inadvertent destruction, among other things.

PI owned by customers is maintained in paper and electronic format in your office and our offices. You should have the following controls in place to safeguard this information: ***Guidance: Select all safeguards***

that currently apply in your business and add information regarding your specific safeguards and practices. Note that you must have strong controls in each of these categories.

- **Physical Safeguards** – you ensure that our premises are secure through use of
    - Locks
    - Alarms
    - Fire suppression
    - Access cards
    - Paper files holding PI are kept in locked file cabinets
    - Reception areas
    - Other

- **Operational Safeguards**

  You have:

    - a clean desk policy.
    - policies and procedures regarding information security.
    - policies and procedures regarding access to PI in work-at-home arrangements.
    - Record retention and destruction schedules: (Note that you must retain customer records according to insurers' records retention policies).
        - You prohibit the removal of PI from your offices.
        - You train staff on information security and the need to safeguard PI.
        - You provide access to PI on a need-to-know basis, generally based on the roles that staff performs.
        - You regularly backup electronic records and provide for their secure storage.

- **Technological Safeguards**

    - Your computers are programmed to scan for viruses.
    - You use encryption for transmission of all sensitive information by electronic means.
    - You have rules for the use of faxes and fax equipment is housed in a protected location away from public view.
    - You ensure the use of passwords on your computers.

Assessing the Program

Guidance: Before establishing a privacy compliance program, you need to do some preliminary assessments. The OPCC suggests starting with a personal information inventory, using a spreadsheet to identify what kind of personal information is collected and where it is kept within/outside of your office. See Appendix E, Personal Information Inventory Worksheet, which you can modify and use for this purpose. It has been pre-populated with information that would typically be found in a Producer's files. See also Appendix F, a Privacy Questionnaire provided by the OPCC, which has been appropriately modified for use by Producers, for an easy-to-use checklist to guide you through the inventory process.

You must assess your controls as often as necessary but in no event less often than every two years, which allows you to develop a gap analysis. This in turn identifies where you have found weaknesses and allows you to create an action plan and timetable for resolution.

Guidance: Appendix G – PIPEDA Self-Assessment Checklist – is modified for Producer use from a document provided by the OPCC. This can form the basis for your regular self-assessments once you have set up your privacy program. Remember to retain documentation of your assessments.

Training

The OPCC urges organizations to train their front-line and management staff and keep them informed, so they can answer the following questions:

- How do I respond to public inquiries regarding our privacy policies?
- What is consent? When and how is it to be obtained?
- How do I recognize and handle requests for access to PI?
- To whom should I refer complaints about privacy matters?
- What are the ongoing activities and new initiatives relating to our protection of PI?

You should receive annual training on privacy issues. See Appendix H, CAILBA's PowerPoint training for Producers. You should supplement this training with other material.

Privacy Breaches

Guidance: The information provided below relates to privacy breaches under PIPEDA. Be aware that some provinces with "substantially similar" legislation have notification requirements. You must be aware of the specific provincial requirements where you do business.

A privacy breach occurs when there is an unauthorized access to, or collection, use or disclosure of PI that contravenes privacy legislation. Typically breaches occur because PI is lost, stolen, disclosed in error or as a consequence of an operational breakdown.

Procedure to Follow for Privacy Breaches:

- **Gather information** about the incident:
  - Date of occurrence
  - Date discovered
  - How discovered
  - Location of the incident
  - Cause of the incident
  - Any other information you can quickly assemble

- **Contain the breach** immediately – don't let any more information escape.
  - Stop the unauthorized practice
  - Recover the records
  - Shut down the system that was breached
  - Revoke or change computer access codes or
  - Correct weaknesses in physical or electronic security.

- **Assess the breach** –The OPCC states that "if the breach appears to involve theft or other criminal activity, notify the police. Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action."

- **If customer information was involved, notify the MGA and determine 1. Who will notify the insurers involved and 2. Who else needs to be apprised** of the incident internally and externally. Depending on

the nature of the breach, the insurer, MGA and Producer should consult on whether affected individuals should be notified, how they will be notified and by whom. The OPCC states "Typically, the organization that has a direct relationship with the customer, client or employee should notify the affected individuals, including when the breach occurs at a third party service provider that has been contracted to maintain or

process the personal information." The decision as to whether to notify the affected individuals may have to be delayed in order for a full risk assessment to be conducted.

- **Evaluate the risks** associated with the breach. Find out:

  a. What PI was involved
  b. How sensitive the information is. Generally, the more sensitive the information, the higher risk of harm. Consider these high risk forms of PI:
     - Health information
     - Government-issued ID such as SINs, driver's licence and health care numbers
     - Bank account and credit card numbers
     - If a ***combination of PI*** was involved, as this is typically more sensitive. The combination of certain types of sensitive PI along with name, address and DOB suggest a higher risk.
  c. How this PI can be used. Can it be used for fraud or other harmful purposes (i.e. identity theft, financial loss, loss of business or employment opportunities, humiliation, damage to reputation or relationships)?
  d. Is there a reasonable risk of identity theft or fraud (usually because of the type of information lost, such as an individual's name and address together with government-issued identification numbers or date of birth)?
  e. Is there a risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment)?
  f. Is there a risk of humiliation or damage to the individual's reputation (e.g., the PI includes mental health, medical or disciplinary records)?
  g. Whether the PI was adequately encrypted, made anonymous or otherwise not easily accessible.
  h. What is the ability of the individual to avoid or mitigate possible harm?
  i. The cause of the breach.
  j. The extent of the breach – how many individuals have been affected?
  k. Who are they?
  l. What harm can result to the Producer and MGA? (Loss of trust, assets, financial exposure, legal proceedings).

- Do a thorough post mortem in order to prevent future breaches. What steps are needed to correct the problem? Is this a one-off issue or is it systemic?

Regulatory Audits of PI Management Practices – What to Expect

Section 18 of PIPEDA permits the OPCC to conduct audits if it has "reasonable grounds" to believe that an organization is contravening PIPEDA. You must receive reasonable notice of an intended audit. Typically, you would receive a letter from the OPCC notifying us of a complaint or plan to audit, along with the name of the person responsible for the file. The letter will ask the name of the PC Officer and will ask for initial documentation by a certain deadline. If you receive such notice:

- Contact the MGA's PC Officer immediately. You may also wish to contact your own legal counsel and seek direction regarding safeguarding solicitor-client privileged information and whether other parties need to be notified of the investigation or audit.

Note that it is an offence to obstruct an investigation, including concealing information, providing misleading information or refusing to provide information. If it is determined that the complaint or investigation is related to the use of customer information, it is very likely that the insurer(s) whose customer information is involved will need to be notified and kept apprised.

- After receiving the initial information, the person named by the OPCC will communicate in writing or by phone to you
  a. How he or she intends to proceed, identifying certain records to review and staff members to interview.
  b. Any dates and times for on-site visits, (which can generally be negotiated).
  c. You must make every effort to determine the cause and the details and scope of the investigation, including what topics will be covered in staff interviews. This is necessary in order to determine what documentation is required, to allow time to locate and analyze the records and to prepare staff who will be interviewed. (Staff must be well-prepared to respond with the appropriate level of information when called upon to do so without venturing opinions, conclusions or unnecessary information).

- During the audit or investigation:
  a. The investigator will likely review your privacy procedures and records related to the investigation and meet with designated staff. Make every effort
  1. to ensure that you can attend any interviews with staff, although the investigator has the right to meet with individuals in private and you must cooperate with these requests.
  b. Document all of the details of the investigation, including the auditor's actions, comments and requests along with the material reviewed and the persons interviewed. Gaining more information about the nature of the complaint or alleged non-compliance that gave rise to the investigation is important.
  c. While the investigator is entitled to review virtually any record in any format, special care must be taken with any material identified as privileged. You may require legal advice in this regard.
  d. If the investigator requests access to original documents, you must ensure that you retain a copy. (All such documents must be returned to you within 10 days if removed from the premises).
  e. If the nature of the complaint or concerns allows for it, you should actively try to resolve the complaint informally and without publicity, seeking an alternative to the OPCC issuing an investigative report.

- Following the audit or investigation:
  a. Before finishing the investigation, the investigator should disclose tentative findings. You should continue to try to resolve the underlying issues before the investigation is finished.
  b. The OPCC is required to provide a report to you, which contains the findings and any recommendations.
  c. It is critically important for you to consider whether the investigation and resulting findings arose as a result of systemic problems and/or failure to adhere to your policies and procedures. An action plan will be required, along with a timetable for resolution of any issues identified.

Contact Information - Regulator

Office of the Privacy Commissioner of Canada

Website: www.priv.gc.ca

This website contains extensive contact information for all provincial privacy regulators and ombudsmen. It is kept up to date and should be our first source of regulatory contact information.

General Inquiries: Toll-free: **1-800-282-1376**
Phone: **(613) 947-1698**
Fax: **(613) 947-6850**
TTY: **(613) 992-9190**
Hours of service are from 8:30 a.m. to 4:30 p.m.

Publication Requests: When requesting publications via e-mail, include your name, telephone number, and return address in order to ensure a reply. Direct your publication request to publications@priv.gc.ca.

To report a breach:
By e-mail: notification@priv.gc.ca;
By phone: 613-995-2042; or,
By mail: Notification Officer
Office of the Privacy Commissioner of Canada
112 Kent Street
Place de Ville
Tower B, 3rd Floor
Ottawa, Ontario
K1A 1H3

Needs-Based Selling

Background

Under numerous provincial rules and insurers' codes of conduct, Producers are required to identify the needs of their customers before making any product or concept recommendations. While Producers tend to do a good job of assessing client needs and matching customers and products, a significant number of Producers fail to adopt a systematic approach by using formal tools that allow them to document their fact finding and needs assessments. This leaves them vulnerable when there are consumer complaints or regulatory and insurer inquiries. In the absence of documented proof of having met the obligation to engage in needs-based selling practices, there will be a predisposition to place more weight on the customer's recollections.

Having a documented needs analysis and complete client file is not a nice-to-have; it's an absolute necessity for any person providing advice and product recommendations in the financial services. The insurers' and regulators' expectation is that Producers be able to demonstrate concrete proof of their sales practices.

In 2006, CCIR (the Canadian Council of Insurance Regulators) and CISRO (the Canadian Insurance Regulators' Organization comprised of provincial insurance councils) endorsed 3 principles for managing conflicts of interest. Among the principles was the idea that any recommended product must be suitable to the needs of the customer. The CCIR agreed that the industry should take the lead in developing a response to the principles.

In 2007, the CLHIA, CAILBA, Advocis and the IFB collaborated on a document titled "The Approach: Serving the Client Through Needs-Based Sales Practices," which is found in Reference Materials**.** It offers guidance on the types of information that you might need to collect or provide. The Approach is an important document that represents the consensus of industry stakeholders about what is required. It is principles-based and flexible and allows the Producer to make decisions about how best to approach the requirements.

Important Note: While The Approach offers the possibility that a needs assessment might not be necessary if the customer identifies his or her needs and approaches the Producer, this apparent carve-out is likely intended for agents selling simple products in non-face-to-face channels such as inbound call centres specializing in term insurance sales. Producers who place business through CAILBA members are considered to be in the face-to-face channel. With very rare exception, they should be completing documented needs assessments on their customers, particularly given anti-money laundering requirements to identify the customer. There have been instances where Producers have asked customers to sign documents "waiving" a needs assessment. It should be noted that customers cannot waive Producer obligations. In fact, the presence of such a letter acts as a red flag for compliance officers and others and will often lead to an investigation of the underlying sale.

Form of Needs Assessment – The CAILBA members through which you place business may offer needs analysis templates on their websites and training on needs-based selling as a service to their Producers. It is unlikely that they will attempt to dictate the form of your needs assessment, since this is a professional's personal choice and should reflect the unique character of his or her practice. There are any number of excellent templates available free of charge on the internet and through various organizations and insurers. Additionally, if you do financial planning and use planning software, it is highly likely that you will be able to easily produce an appropriate documented needs analysis.

Suitability and Appropriateness of Recommendations – with the exception of Quebec and Saskatchewan, which place some responsibility on MGAs for Producers, the suitability of product and advice belongs to the Producer.

However, given the seriousness of the issue and the fact that is a provincial requirement in a number of places, MGAs may be required under their contracts to ensure that you have the tools necessary to do proper needs assessments. Indeed they may be required to audit or spot check files to ensure this is going on. Further, they may ask you to provide samples of the material you use for their records.

The Regulatory Environment – At the time of this writing, the CCIR has published a discussion paper on the regulation of MGAs. It is currently receiving stakeholder input. At some future date, the CCIR may recommend legislative and regulatory changes to the current distribution landscape. This could include rules or guidelines around supervision of Producers and suitability reviews of their recommendations by insurers and/or MGAs.

MGA contracts with Producers may ultimately require Producers to perform documented needs analyses that satisfy the principles laid out in "The Approach" prior to making recommendations to customers. The contracts may reserve the right to review Producers' customer files from time to time to ensure that this requirement is being met. Some MGAs will provide a copy of The Approach in contracting packages.

Required Disclosures

In 2005, in response to high-profile legal and regulatory events in the United States and Canada, the CLHIA, CAILBA, Advocis and IFB collaborated on reference documents for advisor disclosures in individual and group sales. These documents are found in Reference Materials**.** They provide helpful information on the things that Producers should consider, along with sample disclosure letters. The required written disclosures include:

1. Listing all of the insurers that the Producer represents;
2. The nature of the relationship with the companies represented, including any ownership interests or other potential conflicts;
3. How the Producer is compensated;
4. Eligibility for additional compensation such as travel for such things as volume of sales or contests;
5. Any potential or real conflicts of interest;
6. The fact that the customer or plan sponsor has the right to ask for more information.

As with needs analyses, it is extremely advisable that you keep signed copies of these disclosures and provide a copy to the MGA if asked. If you certify to having provided disclosures that you did not in fact provide, this could be grounds for contract termination.

Segregated Fund Disclosures

- A Producer who sells a segregated fund is required to:
  - Deliver the Information Folder and Fund Facts documents for each segregated fund available under the contract to the customer before he or she signs the application for the IVIC. The customer may choose to receive these disclosure documents either physically (in person, mail, or fax) or electronically (e-mail or viewed by the client on-line).
  - Require the customer to sign acknowledging receipt of these documents. (It is advisable to require a copy of this receipt for your files).
    - Ensure that the customer is aware of the rescission right provided by the insurer.

See Reference Materials –CLHIA Guideline G2, Individual Variable Insurance Contracts (IVICs) Relating to Segregated Funds.

The Manitoba Insurance Council offers excellent guidance on what Producers need to know when selling segregated funds. This guidance is reproduced here. It applies to sales throughout Canada.

"It is reasonable for consumers to expect that the agent has the education and expertise to advise them with regard to the investment of their funds. Selling individual variable insurance contracts without the requisite knowledge and expertise may put the agent in jeopardy of disciplinary action or litigation. Information specific to the strategy and product must be provided to the consumer to enable them to make an informed decision. The knowledge required includes the items below:

- <u>About Investing:</u>
  Principle of Risk and Reward
  Assessing Risk Profile
  Asset Allocation and Diversification
  Different types of risk
  Risk measurement tools
  Regulatory Requirements

- <u>About the Consumer:</u>
  Investment Objectives
  Risk Tolerance
  Investment Time Frames
  Investment Knowledge
  Assets and liabilities
  Amount available for investment

- <u>About the Individual Variable Investment Contract:</u>
  Maturity Guarantees available
  Death Benefit Options available
  Other guarantees available (e.g. GMWB)
  Costs associated with the contract
  Costs associated with the guarantees
  Volatility of potential returns
  Impact of withdrawals on any guarantees
  Sales charges (e.g. up front, deferred, no load)
  Resets available
  Funds available within the contract
  Tax implications associated with the contract
  Rights if consumer should decide to rescind the contract (time frames)
  Costs if contract is surrendered

- <u>About the Funds Available Within the Contract:</u>
  Investment philosophy and objective of Fund Manager(s)
  Amount and type of risk in each fund
  Investments held by the fund (e.g. top 10 holdings)
  Fund past performance
  Technical details of fund (e.g. age, size, turnover rate)

- <u>How the Consumer can get additional information or assistance:</u>
  Information available in Information Folder
  Fund Statements

Company Website
1-800 phone number
Company Client Service, Ombudsman, Regulatory body

DOCUMENTATION/RETENTION
Documentation must be retained should it ever become necessary to verify that all the proper steps were taken in making the recommendations. At a minimum the following documentation should be retained in the agent's files:

Documentation of consumer contact(s)
Documentation of consumer's risk tolerance, time horizon, investment knowledge and objectives
Documentation which supports a leveraging strategy, if applicable, and client acknowledgement of risks
Documentation of transaction instructions and authorization and detailed notes of client meetings and discussions."

Do Not Call List

Producers who engage in telemarketing either directly or through others are subject to the CRTC's Unsolicited Telecommunications Rules, including National Do Not Call List "N-DNCL." They may not attempt to telemarket to numbers that are on the N-DNCL without express prior consent. The Producer must understand the extensive rules and understand that he or she is required to register with the N-DNCL Operator, who registers consumers' numbers for the list, provides telemarketers with updated versions of the list and receives consumer complaints about calls. ***Referrals are not exempted because the required consent has not been received.*** Currently, there are no fees for registering but there is provision for fees at a future date.

Exclusions and Exemptions from the N-DNCL:

Service Calls
The N-DNCL rules do not apply to service calls from a Producer, which consist of calls that relate to advice, products or services the client or prospect has purchased, applied for or inquired about, along with any calls that are required by regulation or standards of professional conduct.

Existing Business Relationship

A Producer has an existing business relationship with a person if that person has:

- Purchased goods or services from the Producer within the last 18 months;
- Inquired about insurance or applied for a product or service within 6 months of the call or
- If the customer has a written contract in effect or expired within 18 months of the call.

There appears to be quite a lot of latitude for a Producer to maintain contact with his existing customers and prospects. How he or she acquires those prospects in the first place is what is at issue. Given the advent of social networking media and other means of communication, restrictions on prospecting for clients or acting on referrals by telephone appear to be manageable. **See Reference Materials - CLHIA Guidance on CRTC Do Not Call List.**

Records and File Management

Records management has become a hot button issue with OSFI and the Federal and provincial privacy authorities, although for different reasons. Insurers are actively building out their records management policies and procedures and will without question turn their sights to their distributors in their risk assessments. Your MGA may perform spot checks or audits of your practices and may be able to help you to identify and repair poor record-keeping practices. Well-maintained files are a Producer's best protection.

Customer files should contain enough information to demonstrate that a needs-based sale took place. A well-maintained file should contain copies of the material that (or detailed notes on what) was provided to the customer.

While Producers are required to verify client ID in keeping with federal AML laws, unlike the rules around the sale of mutual funds, there is no requirement to retain actual copies of the customer's personal ID in insurance files. Much of the information contained on that personal ID must be retained, however.

Review your files regularly to identify records that are due for destruction.

A Customer file should contain the following and should be retained:

1. Needs analysis, any financial plan and investor profile
2. Copies of dated illustrations shown to customer.
3. Any email or letter communications with customer
4. Dated notes on any discussions in person or via telephone
5. Copies of any completed forms
6. Policy delivery receipt, where required
7. Any customer complaint documentation. (In Quebec, this must be maintained as a separate file).

The following items should not be found in customer files:

1. Original undelivered policy.
2. Any pre-signed blank forms.
3. Client copy of confirms or correspondence
4. Any medical information, including medical portion of application, lab tests or physician notes (all such documentation should be shredded immediately upon policy issuance).
5. Documents pertaining to other insurance policies or mutual funds (each should be held in separate files. They should not be subject to review by mutual fund regulators or insurers unrelated to the policy in question.

Complaints Management

If you are a Producer in Quebec or hold a licence in Quebec, there are certain requirements to which you must adhere, including the establishment of a complaints protocol. You must be aware of these requirements.

You are required by the CAILBA Producer Code of Conduct to maintain a Complaint log that includes:

- Customer name

- Policy or document number
- Producer name
- Date of complaint, (written or verbal)
- Recipient of complaint
- Individual handling the complaint
- Summary of complaint (details should include whether a regulatory body is involved.)
- Whether the complaint was reported to the insurer and/or MGA and the contact information.
- Steps towards resolution
- Statement of resolution and date of resolution.

It is vitally important that you keep this log in good order. It is a protection for your business. You may be called upon to produce the complaint log in regulatory and insurer audits.

Responding to Insurance Company Requests

Many insurers' contracts require you to cooperate and be responsive to requests for information. Contracts also generally call for cooperation and assistance in responding to complaints or investigations into business practices or conduct. Insurers typically expect to be provided access to your records related to all matters governed by the contract. Failure to cooperate can be grounds for contract termination and in some cases, reports to regulators.

Regulatory Audits and Inquiries and Legal Proceedings

Some insurers' contracts require you to notify them of any interactions you have with regulators, in particular any enforcement actions or legal proceedings. It is critically important that you notify your errors and omissions insurance carrier as well. Depending on the nature of the audit, inquiry or proceeding, you should consider contacting your outside legal counsel for direction and assistance.

Membership in Professional Associations

The concept of "independent producer" is virtually unheard of in the other financial services and participants from rules-based regimes tend to look askance at the structure of distribution in the life insurance business. At the same time, there is no evidence that the end consumer is less protected or less well-served in our sector. However, independence comes with some strict obligations, including development of your own AML, privacy and market conduct programs, policies and procedures.

CAILBA has provided this guidance manual to you as a courtesy to assist you in building your compliance program. It is your obligation to take action and do the things you are required to do by regulation. Your MGA is there to assist.

Membership in a professional association like CAILBA or IFB offers even more assistance. For one thing, most insurers, regulators and MGAs would consider professional membership to be a form of "control." It counts as a positive in assessing a Producer's suitability.

Membership has other distinct advantages. Professional organizations strive to make information about regulatory and legislative changes available to members, in part to keep them current and in part to ensure that members have an opportunity to weigh in on matters that concern them. Associations exist to protect and advance their members' interests. They also offer continuing education, networking opportunities and professional development. If you are not currently a member of an association, it is wise to investigate your choices and give thought to joining.