Canada Financial®

Our Strength is Our People

www.canadafinancial.ca

Compliance Manual

Last Revision: March 7, 2017

Table of Contents

Introduction

The successful implementation of high standards of compliance is a crucial factor that contributes to the continued success of, and public confidence in, life insurance companies and advisors doing business in Canada. The establishment and implementation of an effective compliance program will determine how we are perceived by various stakeholder groups with the financial industry, including our clients, the advisors, the policyholders, our employees, our suppliers, regulators and the public at large. These stakeholders are aware that higher standards of compliance are increasingly being expected of both private and public Canadian companies.

The objective of this manual, therefore, is to clarify and promote compliance excellence within our organization through:

(i) High standards of competence, accountability, and disclosure
(ii) Compliance with legal regulations
(iii) Consistency with best corporate governance practices

Recruiting and Selection

EXPERIENCED

1. 1st interview: Introduction/ Promotion
2. 2nd interview: Expectations/ Screening Challenges/ Expectations/ P100
3. 3rd interview: Decision (Subject to following)
4. Green Grass Report Ordered
5. Evaluation: Do not hire if compliance record Debit with carrier production (20,000 FYC/year+). Integrity/ Discipline 2 transfers + in past 3 years Credit and Criminal Record (IC of BC)
6. Expectation to (5) investigation of compliance record by Chief Compliance Officer
    a. No exception for debit
    b. Less than required production or excessive transfers
    c. Provide formal business plan
    d. Discuss with VP or CEO

NEW TO THE INDUSTRY

1. 1st interview/ seminar: sell the career
2. 2nd interview: Expectations/ Screening Challenges/ Expectations/ P100
3. 3rd interview: Review P100/ Decision
4. 4. LLQP or Mentoring Program
5. Evaluation Achievements (from Resume)

Financial Solvency

Our current regulatory environment requires all professionals involved with the financial services industry to maintain the highest standard of compliance constantly.

All contracts with insurance carriers that an Advisor has requires that the Advisor complies with each carrier's policies as specified in each contract, and also require that such carrier ensures that their contracted Advisors comply with the requirements of the Insurance Act and the regulatory environment in the Province or Territory in which you operate.

One of the responsibilities that belong with the holding of these insurance representation contracts is the continuing financial solvency of the licensed practitioner; regulators also require notifications of solvency problems.

A licensee must notify the Insurance Council of BC within 5 business days where the licensee or any business the licensee owns or has participated in as a director, officer or partner:

1. Disciplined by any financial sector regulator, or any professional or occupational body;
2. Declares bankruptcy
3. Has any judgment rendered about any insurance activities, fraud or breach of trust; or;
4. Is charged or convicted of any criminal offense or any offense under law or any jurisdiction, excluding traffic offenses resulting in monetary fines only.

More specifically, some of our carrier's solvency policy prevents the continuance of a representation contract in the events of bankruptcy declaration or entering a consumer proposal.

All advisors need to inform:

1. The Insurance Council,
2. All contracted insurance carriers and
3. CF Canada Financial Group Inc.

in the event of such occurrences, within 5 business days.

Guidelines for Marketing Materials

Our current regulatory environment requires all professionals involved with the financial services industry to maintain the highest standard of compliance constantly.

One of the key responsibilities relates to the holding out to the public with regards to the products and services we offer. One important part of this holding out refers to any printed or electronic material describing or representing the nature of such products and services.

It is imperative that any such material never contains any intentional or unintentional misrepresentation or misleading information.

It is strongly advisable to follow CF guidelines in the printing of your business cards.

In the case where another material is concerned, CF recommends limiting the distribution of such materials to the printed and approved publications of our carrier companies which are widely available from the CF offices and the carriers themselves.

Further, any use of company logo or trademark requires the approval and consent of the companies themselves and must be submitted in writing to the companies for approval.

In no case should these logos and trademarks or company references be used without the express approval and consent for each specific usage.

Monitoring and investigation

CF Canada Financial will maintain a regular monitoring process through its internal procedures and through its staff to ensure that compliance procedures are maintained in all its operations and the operations of the Independent Advisors that submit business through CF Canada Financial.

While responding to all complaints brought to the attention of CF Canada Financial and its staff, our process will monitor indicators of possible compliance issues other than complaints:

Some of these indicators will be:

1. Missing/suspicious/inappropriate signing of documents
2. Missing/inappropriate witnessing
3. Suspicious/missing ID
4. Cash transactions
5. Excessive replacement activities
6. Excessive lapses
7. Signed blank forms
8. Unlicensed advisors
9. Evidence of fronting

9.1.1. **Definition**

There are two kinds of Fronting:

1. The Advisor submits an application on behalf of another licensed person who is not authorized to represent that particular company
2. The Advisor submits an application on behalf of an unlicensed person.

Note that some Carriers – such as Manulife – have specific policies regarding fronting**:** Manulife advisors are prohibited from engaging in the practice of fronting. In circumstances where more than one Manulife advisor has participated in making representations to a client in a particular sale, both advisors' names and codes should be recorded on the application in the space provided. Manulife advisors must ensure that any other individual who is representing a Manulife product to their client is life insurance licensed and authorized to represent Manulife.

In addition to monitoring indicators, CF will perform random checks for valid Licenses and valid E&O.

Complaint Handling Procedures

The following outlines CF Canada Financial policies and procedures for dealing with complaints to ensure that complaints are dealt with promptly and fairly.

A "complaint" is deemed to include an alleged grievance involving CF Canada Financial or a CF Canada Financial Advisor in the form of:

1. Any written statement, including electronic communications, of a client, or any person acting on behalf of a client, or of a prospective client involving matters that occurred while the Financial Advisor was contracted with CF Canada Financial

2. Any written or verbal statement from any person alleging:

2.1. Theft, fraud, misappropriation of funds or insurance, forgery, money laundering, market manipulation, insider trading, misrepresentation, or unauthorized trading;

2.2. Insurance related business outside of CF Canada Financial;

2.3. An undeclared conflict of interest arising from an occupation outside of CF Canada Financial;

2.4. Personal financial dealings with a client;

3. Any other verbal statement of grievance from a client for which the nature and severity of the client's allegations will warrant, in the professional judgment of CF Canada Financial' supervisory staff handling the complaint, the same treatment as a written complaint.

Send Complaints to:

CF Canada Financial

1188 – 1095 West Pender Street

Vancouver, BC

V6E2M6

Attention: Compliance Officer

To ensure that CF Canada Financial provides an equitable process for the handling of complaints, the following process has been established:

Responding to Complaints:

1. Ensure that your area is the appropriate area to handle the complaint. If not, immediately refer to your direct Manager and CF Compliance Department

2. An acknowledgment letter (Appendix C) is to be sent to the complainant within a maximum of 10 days (ideally, within 5 days) of receipt of the complaint;

3. CF will strive to resolve the complaint within 45 days from the date it was received. A complainant is to be informed no later than 15 days after a complaint has been dealt with, the reasons for the decision reached, the details of any proposed resolution as well as details of further avenues available for the person i.e. external dispute resolution bodies available.

4. Upon receipt of a written complaint or a verbal statement of grievance, CF Canada Financial' Compliance Department will (i) immediately record the complaint in the complaint log; and If the complaint cannot be handled immediately (investigation required), CF will send an initial response letter in the form attached as Schedule "A" within five (5) business days of receipt of the written complaint.

5. CF Canada Financial will notify the applicable CF Canada Financial Advisor and respective Manager about the complaint and, where appropriate and/or possible, request their information and documentation with respect to the complaint.

6. Where the complaint involves allegations of serious misconduct, breach of privacy or is a legal action, CF Canada Financial' Compliance Department will make senior management aware of the complaint.

7. In all such cases, if the complaint involves (a) the business of one of CF's contracted Product Provider Companies or (b) the suitability of the contracted advisor, CF will notify the Provider Company Compliance Department about the complaint.

8. CF Canada Financial' Compliance Department will commence its investigation and analysis of the allegations raised in the complaint with intending to provide a substantive response to the client or individual within 90 days of receipt of the written complaint.

9. With respect to the investigation and analysis, CF Canada Financial' Compliance Department will gather the facts, information and documentation where possible from the applicable and/or available sources within CF Canada Financial and/or elsewhere and objectively consider the complaint.

10. Complaints will not be dismissed based on any predetermined factors; rather each complaint will be considered individually on its own merits. In gathering the facts, CF Canada Financial may contact the client or individual to request additional information required to resolve the complaint.

11. Once the investigation has been completed, the substantive response letter will be prepared.

12. Depending on the nature of the alleged grievance, the proposed response will be reviewed by CF Compliance Department and if appropriate, CF's Executive Management.

13. Each substantive response letter will include an outline of the complaint and CF Canada Financials substantive decision on the complaint, including the reasons for the decision.

14. CF Canada Financial' substantive response letter will be sent to the client by regular letter mail or, in some instances, by courier. CF Canada Financial will continue to proactively address further communication from the client or individual as appropriate in a timely manner until no further action is deemed to be required by CF Canada Financial in its professional judgment.

Schedule "A"

[CF CANADA FINANCIAL LETTERHEAD]

[Date]

[Client Name

Address]

Dear Client Name:

CF Canada Financial acknowledges receipt on [Month, Day, Year] of your letter of complaint dated [Month, Day, Year].

We are investigating your complaint and will respond to you with the results of our investigation. CF Canada Financial endeavors to provide substantive responses to client complaints within 90 days of receipt. This timeline may be extended where we have requested additional information from you or if your complaint requires an extensive amount of fact-finding or complex legal analysis. In instances where the timeline is extended, CF Canada Financial will keep you apprised of the status of your complaint.

[Include request for any additional reasonable information required to resolve the complaint if known at this time]

If at any time you would like to inquire about the status of your complaint or provide CF Canada Financial with any additional information or documentation relating to your complaint, please feel free to contact me at the mailing address noted below, by [telephone, fax and e-mail co-ordinates].

Yours truly,

[Name]

Manager, Complaints, and Regulatory Investigations encls.

Code of Conduct

CF Canada Financial expects all CF contracted advisors to follow the Code of Conduct of the Province(s) and Territories the advisors are licensed .

In addition, advisors are expected to also follow the Codes of Conduct as required by their contractual obligations with the Carriers they hold contract with and represent in the field.

Disclosure at Point of Sale

There are six types of information that require WRITTEN DISCLOSURE to the client at the time of sale:

1. Company(ies) with which the advisor places or recommends business

2. Nature of relationship with insurer(s) providing product

3. How the advisor is compensated

4. If the advisor may be eligible for additional compensation (cash or nonmonetary, such as qualifier conferences)

5. Conflicts of interest

6. Other information that you might wish to include:
   a) license(s) held
   b) signature of agent
   c) signature of client

Disclosure is often addressed in the application forms printed by insurance carriers, however it is often in the form of an assertion that such information has been separately provided to the client (example: CL Life application, paragraph 15.13 at the bottom of "advisor report") thus leaving the agent still responsible for providing the information in writing.

While a basic disclosure statement can be obtained from the CLHIA website, CF Canada Financial provides advisors with two sample engagement letters that contain the required information as well as the standards of engagement with a client and a positive marketing message to qualify the Agent's professionalism.

Continuing Education

All Life Insurance licensees are required to meet the continuing education requirements outlined below for each license year. A license year runs from 01JUN to 31 MAY annually. If a licensee has been licensed for any part of a license year, the individual must meet the full number of continuing education requirements, whether the license was active or inactive.

Below is information on a licensee's requirement to maintain records and on Council audits. At the end of this page are links to each of the continuing education programs (hours and type of education required) for each class of license.

If you are a non-resident of British Columbia, you must meet the same requirements as a resident, with some exceptions and additions. Read this NON-RESIDENTS Information Page.

Requirement to Maintain Records

- Licensees must ensure they have a valid record of course completion. Check with the course provider in advance to see if one is provided. If not, bring a form with you and ask the facilitator to sign it at the end of the session. When attending a conference with a number of different seminars, bring a summary sheet listing seminar titles, dates and hours and have each presenter sign at the end. A payment receipt will not be considered proof of attendance. You must have attended the full seminar or course.

- Keep your proof of attendance records in a specific continuing education file, along with sufficient information on how the credit hours were determined. This includes topic outlines, the presenter's name and qualifications and the times and dates. Some of this information may be in the course material.

- Records to support continuing education must be kept for five years from the end of the license period for which the education was used. Random audits are conducted. If you do not have the supporting documentation, Council may take disciplinary action, including invalidating the license filing.

Continuing Education Audits

When audited, licensees will be asked to provide proof of completion or attendance for the continuing education taken. Original proof of attendance records will be required. Where a course or seminar was given by other than a RECOGNIZED EDUCATION PROVIDER, licensees must include sufficient information for Council to determine the content and length of the education as required under the Continuing Education Program. Licensees are expected to make a timely response to audit requests. Once the audit is completed, all original documents will be returned.

Life Insurance Continuing Education

1. Number of Hours Required:

For each license year or portion thereof, commencing with license year 01JUN2008 through 31 MAY 2009:

- if you have an approved designation* you must have 5 technical hours of continuing education; OR
- if you have been licensed as a life insurance agent for at least 5 of the last 7 years in a Canadian jurisdiction, and you do not have an approved designation you must have 10 technical hours of continuing education; OR
- if you have not been licensed as a life insurance agent for at least 5 of the last 7 years in a Canadian jurisdiction and you do not have an approved designation you must have 15 technical hours of continuing education.

*Approved Designations: CFP, CLU, RHU, FCIA, FLMI and CEBS. Designations from other countries will be considered where it is demonstrated to Council they are equivalent to one of the approved Canadian designations.

NOTE: Some designations (CLU, FCIA, and CFP) require the holder to keep the designation in good standing by completing continuing education each year. If you hold such a designation and can demonstrate to Council your designation is in good standing, you are "exempt" from Council's continuing education requirements.

2. Content:

The only technical material will qualify for continuing education. Technical education directly relates to:

- life insurance products;
- financial planning provided the education is geared to life insurance and not a non-insurance sector, such as securities or mutual funds;
- compliance with insurance legislation and requirements such Council's Code of Conduct, Council Rules, the Insurance Act, privacy legislation and anti-terrorism/money laundering legislation; ethics; or E&O.

3. Structure:

The education must take place in a structure dedicated to learning. Day-to-day business or professional reading does not qualify. However, a separate training meeting to review the details of a specific product line may qualify, but regular staff meetings that cover a myriad of topics do not.

4. Facilitator:

The facilitator is expected to be fully qualified. You can usually verify this through a course or promotional materials.

5. Time:

One hour of instruction is equal to one hour of continuing education credit, subject to a one hour minimum. Breaks are excluded and you must attend the complete course or seminar. In addition:

- no course can be accredited for more than 15 hours;
- there is a daily maximum of 7 hours; and
- where a course involves an exam, you must successfully pass the exam.

6. Carry Forward

Commencing 01JUN2008, excess credits cannot be carried over into the next licence period.

Privacy Principles and Procedures

CF Canada Financial will endeavor to respect and maintain the privacy and confidentiality of all personal information collected as part of the requirements of conducting our Insurance and Financial business.

We will abide by the ten principles of privacy as quoted in the guidelines by the Office of the Privacy Commissioner.

Further, we will follow our documented Complaint Handling Procedures to resolve any complaint, issue, and grievance.

Where appropriate, if the complaint involves allegations of serious misconduct, breach of privacy or is a legal action, CF Canada Financial's Compliance Department will make senior management aware of the complaint.

In all such cases, if the complaint involves (a) the business of one of CF's contracted Product Provider Companies or (b) the suitability of the contracted advisor, CF will notify the Provider Company Compliance Department about the complaint

An organization is responsible for the protection of personal information and the fair handling of it at all times, throughout the organization and in dealings with third parties. Care in collecting, using and disclosing personal information is essential to continued consumer confidence and good will.

The 10 principles that businesses must follow are:

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure, and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

1. Be accountable

Your responsibilities:

Comply with all 10 of the principles of Schedule 1.

Appoint an individual (or individuals) to be responsible for your organization's compliance.

Protect all personal information held by your organization or transferred to a third party for processing.

Develop and implement personal information policies and practices.

2. Identify the purpose

Your organization must identify the reasons for collecting personal information before or at the time of collection.

Your responsibilities:

Before or when any personal information is collected, identify why it is needed and how it will be used.

Document why the information is collected.

Inform the individual from whom the information is collected why it is needed.

Identify any new purpose for the information and obtain the individual's consent before using it.

3. Obtain consent

Your responsibilities:

Inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data.

Obtain the individual's consent before or at the time of collection, as well as when a new use is identified.

4. Limit collection

Your responsibilities:

Do not collect personal information indiscriminately.

Do not deceive or mislead individuals about the reasons for collecting personal information.

5. Limit use, disclosure, and retention

Your responsibilities:

Use or disclose personal information only for the purpose for which it was collected, unless the individual consents or the use or disclosure is authorized by the Act.

Keep personal information only as long as necessary to satisfy the purposes.

Put guidelines and procedures in place for retaining and destroying personal information.

Keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress.

Destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.

6. Be accurate

Your responsibilities:

Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.

7. Use appropriate safeguards

Your responsibilities:

Protect personal information against loss or theft.

Safeguard the information from unauthorized access, disclosure, copying, use or modification.

Protect personal information regardless of the format in which it is held.

8. Be open

Your responsibilities:

Inform customers, clients, and employees that you have policies and practices for the management of personal information.

Make these policies and practices understandable and easily available.

9. Give individuals access

Your responsibilities:

When requested, inform individuals if you have any personal information about them.

Explain how it is or has been used and provide a list of any organizations to which it has been disclosed.

Give individuals access to their information.

Correct or amend any personal information if its accuracy and completeness are challenged and found to be deficient.

Provide a copy of the information requested, or reasons for not providing access, subject to exceptions set out in Section 9 of the Act (see page 18).

An organization should note any disagreement on file and advise third parties where appropriate.

10. Provide recourse

Your responsibilities:

Develop simple and easily accessible complaint procedures.

Inform complainants of their avenues of recourse. These include your organization's 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.

Key Steps to Follow in Responding to Privacy Breaches

1. Breach Containment and Preliminary Assessment
2. Evaluate the Risks
3. Notification
4. Prevention of Future Breaches

Purpose

The purpose of this document is to provide guidance to financial agencies and advisors when a privacy breach occurs. Financial agencies and advisors should take preventative steps before a breach occurring by having reasonable policies and procedural safeguards in place and conducting necessary training. This guideline is intended to help financial agencies and advisors take the appropriate steps in the event of a privacy breach and to provide guidance in assessing whether notification to affected individuals is required. Not all steps may be necessary, or some steps may be combined.

What is a privacy breach?

A privacy breach occurs when there is unauthorized access to or collection, use, or disclosure of personal information. Such activity is "unauthorized" if it occurs in contravention of applicable privacy legislation, such as PIPEDA, or similar provincial privacy legislation. Some of the most common privacy breaches happen when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed (e.g., a computer containing personal information is stolen or personal information is mistakenly emailed to the wrong people). A privacy breach may also be a consequence of a faulty business procedure or operational break-down.

Four key steps in responding to a privacy breach

There are four key steps to consider when responding to a breach or suspected breach:

1) Breach containment and preliminary assessment
2) Evaluation of the risks associated with the breach
3) Notification
4) Prevention

Be sure to take each situation seriously and move immediately to investigate the potential breach. You should undertake steps 1, 2 and 3 either simultaneously or in quick succession. Step 4 provides recommendations for longer term solutions and prevention strategies. The decision on how to respond should be made on a case-by-case basis.

Associated with this guideline is a checklist that financial agencies and advisors can use to help ensure they have made the appropriate considerations in dealing with a possible privacy breach.

Step 1: Breach Containment and Preliminary Assessment

You should take immediate common sense steps to limit the breach..

- Immediately contain the breach (e.g., 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).

- Designate an appropriate individual to lead the initial investigation. This individual should have appropriate scope within the organization to conduct the initial investigation and make initial recommendations. If necessary, a more detailed investigation may subsequently be required.

- Determine the need to assemble a team which could include representatives from appropriate parts of the business.

- Determine who needs to be made aware of the incident internally, and potentially externally, at this preliminary stage. Escalate internally as appropriate, including informing the person within your organization responsible for privacy compliance. 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.

Step 2: Evaluate the Risks Associated with the Breach

To determine what other steps are immediately necessary, you should assess the risks associated with the breach. Consider the following factors in assessing the risks:

(i) Personal Information Involved

- What data elements have been breached?

- How sensitive is the information? Generally, the more sensitive the information, the higher the risk of harm to individuals. Some personal information is more sensitive than others (e.g., health information, government-issued pieces of identification such as social insurance numbers, driver's licence and health care numbers, and financial account numbers such as credit or debit card numbers that could be used in combination for identity theft). A combination of personal information is typically more sensitive than a single piece of personal information. However, sensitivity alone is not the only criteria in assessing the risk, as foreseeable harm to the individual is also important.

- What is the context of the personal information involved? For example, a list of customers on a newspaper carrier's route may not be sensitive. However, the same information about customers who have requested service interruption while on vacation may be more sensitive. Similarly, publicly available information such as that found in a public telephone directory may be less sensitive.

- Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?

- How can the personal information be used? Can the information be used for fraudulent or otherwise harmful purposes? The combination of certain types of sensitive personal information along with name, address and date of birth suggest a higher risk due to the potential for identity theft.

An assessment of the type of personal information involved will help you determine how to respond to the breach, who should be informed, including the appropriate privacy commissioner(s), and what form of notification to the individuals affected, if any, is appropriate. For example, if a laptop containing adequately encrypted information is stolen, subsequently recovered and investigations show that the information was not tampered with, notification to individuals may not be necessary.

(ii) Cause and Extent of the Breach

- To the extent possible, determine the cause of the breach

- Is there a risk of ongoing breaches or further exposure of the information?

- What was the extent of the unauthorized access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online?

- Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?

- Has the personal information been recovered?

- What steps have already been taken to mitigate the harm?

- Is this a systemic problem or an isolated incident?

(iii) Individuals Affected by the Breach

- How many individuals' personal information is affected by the breach?

- Who is affected by the breach: employees, contractors, public, clients, service providers, other financial agencies, and advisors?

(iv) Foreseeable Harm from the Breach

- In assessing the possibility of foreseeable harm from the breach, have you considered the reasonable expectations of the individuals? For example, many people would consider a list of magazine subscribers to a niche publication to be potentially more harmful than a list of subscribers to a national newspaper.

- Who is the recipient of the information? Is there any relationship between the unauthorized recipients and the data subject? For example, was the disclosure to an unknown party or to

a party suspected of being involved in criminal activity where there is a potential risk of misuse? Or was the recipient a trusted, known entity or person that would reasonably be expected to return the information without disclosing or using it?

- What harm to the individuals could result from the breach? Examples include:

 security risk (e.g., physical safety); o identity theft; o financial loss; o loss of business or employment opportunities; or o humiliation, damage to reputation or relationships.

- What harm to the organization could result from the breach? Examples include:
    - Loss of trust in the organization
    - Loss of assets
    - Financial Exposure
    - Legal proceedings (i.e. class action suits).
- What harm could come to the public as a result of notification of the breach? The harm that could result in includes:
    - The risk to Public Health
    - Risk to Public Safety

Step 3: Notification

Notification can be an important mitigation strategy that has the potential to benefit both the organization and the individuals affected by a breach. If a privacy breach creates a risk of harm to the individual, those affected should be notified. Prompt notification to individuals in these cases can help them mitigate the damage by taking steps to protect themselves. The challenge is to determine when notices should be required. Each incident needs to be considered on a case-by-case basis to determine whether privacy breach notification is required. Financial agencies and advisors are also encouraged to inform the appropriate privacy commissioner(s) of material privacy breaches, so they are aware of the breach.

The key consideration in deciding whether to notify affected individuals should be whether the notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately accessed, collected, used or disclosed. Financial agencies and advisors should also take into account the ability of the individual to take specific steps to mitigate any such harm.

(i) Notifying Affected Individuals

Financial agencies and advisors should consider the following factors when deciding whether to notify:

- What are the legal and contractual obligations?

- What is the risk of harm to the individual?

- 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)?

- Is there a risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment)?

- Is there a risk of humiliation or damage to the individual's reputation (e.g., when the information lost includes mental health, medical or disciplinary records)?

- What is the ability of the individual to avoid or mitigate possible harm?

(ii) When to Notify, How to Notify and Who Should Notify

At this stage, you should have as complete a set of facts as possible and have completed your risk assessment in order to determine whether to notify individuals.

When to notify: Notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the breach. However, if law enforcement authorities are involved, check with those authorities whether notification should be delayed to ensure that the investigation is not compromised.

How to notify: The preferred method of notification is direct – by phone, letter, email or in person – to affected individuals. Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost or the contact information for affected individuals is not known. Using multiple methods of notification in certain cases may be appropriate. You should also consider whether the method of notification might increase the risk of harm (e.g., by alerting the person who stole the laptop of the value of the information on the computer).

Who should notify: 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. However, there may be circumstances where notification by a third party is more appropriate. For example, in the event of a breach by a retail merchant of credit card information, the credit card issuer may be involved in providing the notice since the merchant may not have the necessary contact information.

(iii) What should be Included in the Notification?

The content of notifications will vary depending on the particular breach and the method of notification chosen. Notifications should include, as appropriate:

- Information about the incident and its timing in general terms;

- A description of the personal information involved in the breach;

- A general account of what the organization has done to control or reduce the harm;

- What the organization will do to assist individuals and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves. Possible actions include arranging for credit monitoring or other fraud prevention tools, providing information on how to change a social insurance number (SIN), personal health card or driver's license number. For example, to obtain a new SIN HTTP://www1.servicecanada.gc.ca/en/cs/sin/0200/0200_010.shtml;

- Sources of information designed to assist individuals in protecting against identity theft (e.g., online guidance on the Office of the Privacy Commissioner's website HTTP://www.priv.gc.ca/resource/ii_4_01_e.cfm and Industry Canada website athttp://strategis.ic.gc.ca/epic/site/oca-bc.nsf/en/h_ca02226e.html);

- Providing contact information of a department or individual within your organization who can answer questions or provide further information;

- If applicable, indicate whether the organization has notified a privacy commissioner's office and that they are aware of the situation;

- Additional contact information for the individual to address any privacy concerns to the organization; and

- The contact information for the appropriate privacy commissioner(s).

Be careful not to include unnecessary personal information in the notice to avoid possible further unauthorized disclosure.

(iv) Others to Contact

- Privacy Commissioners: financial agencies and advisors are encouraged to report material privacy breaches to the appropriate privacy commissioner(s) as this will help them respond to inquiries made by the public and any complaints they may receive. They may also be able to provide advice or guidance to your organization that may be helpful in responding to the breach. Notifying them may enhance the public's understanding of the incident and confidence in your organization. The following factors should be considered in deciding whether to report a breach to privacy commissioners' offices:

    a. any applicable legislation that may require notification

    b. whether the personal information is subject to privacy legislation

    c. the type of the personal information, including:

        - whether the disclosed information could be used to commit identity theft;

        - whether there is a reasonable chance of harm from the disclosure, including non-monetary losses;

d. the number of people affected by the breach; o whether the individuals affected have been notified; and

e. if there is a reasonable expectation that the privacy commissioner's office may receive complaints or inquiries about the breach.

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or financial agencies and advisors should also be informed of the breach, as long as such notifications would be in compliance with PIPEDA or similar provincial privacy legislation:

- Police: if theft or other crime is suspected.
- Insurers or others: if required by contractual obligations.
- Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies.
- Credit card companies, financial institutions or credit reporting agencies: if their assistance is necessary for contacting individuals or assisting with mitigating harm.
- Other internal or external parties not already notified:
    - third party contractors or other parties who may be impacted;
    - internal business units not previously advised of the privacy breach, e.g., government relations, communications and media relations, senior management, etc.; or o union or other employee bargaining units.

Financial agencies and advisors should consider the potential impact that the breach and notification to individuals may have on third parties and take actions accordingly. For example, third parties may be affected if individuals cancel their credit cards or if financial institutions issue new cards.

Step 4: Prevention of Future Breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, financial agencies and advisors need to take the time to investigate the cause of the breach and consider whether to develop a prevention plan. The level of effort should reflect the significance of the breach and whether it was a systemic breach or an isolated instance. This plan may include the following:

- a security audit of both physical and technical security;
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that (e.g., security policies, record retention, and collection policies, etc.);

- a review of employee training practices; and
- a review of service delivery partners (e.g., dealers, retailers, etc.).

The resulting plan may include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.

The OPC has also developed a checklist based on these four key steps that will help financial agencies and advisors gather all the necessary information and complete an analysis in the event of a privacy breach.

Financial Transactions and Reports Information for Life Insurance

Every country in the world, perhaps with a few notable exceptions, is engaged in finding ways to protect the legitimate financial system from those who would abuse it—finding ways to detect and deter and prevent money laundering and terrorist activity financing.

When it comes to deterrence and prevention, the work that FINTRAC does to ensure compliance with the law strives to keep illicit funds from entering the legitimate Canadian financial system. This involves ensuring that proper records are kept, that identification is obtained, that risks are being assessed and the other elements of a compliance regime are in place.

All the entities that make up Canada's financial system have a stake in ensuring that the level of deterrence is high. Life insurance companies have a stake in this too.

When it comes to detection, FINTRAC's intelligence assists investigations, and it assists prosecutions. Financial Intelligence sheds light on the transactions that can be related to criminal activity. It assists investigators in making decisions about where to seek evidence, who to include or exclude as part of the investigation, how the targets are connected and where the assets may be hidden.

There are specific legislative requirements under the PCMLTFA -Proceeds of Crime (Money Laundering) and Terrorist Financing Act – that apply to life insurance companies, brokers and independent agents.

Information for Life Insurance

Your Obligations

The following summary of the legislative requirements under the PCMLTFA applicable to life insurance companies, brokers or independent agents. If you are a life insurance agent and an employee of a life insurance company or broker, these requirements are the responsibility of the life insurance company except with respect to reporting suspicious transactions and terrorist property, which is applicable to both.

For information about legislative requirements in effect before June 23, 2008, see the applicable guidelines published before 2008.

Note: Content in this section may require additional software to view. Consult our Help page.

Information for: Life insurance (PDF version, 65 kb)

Additional Information for Life Insurance Companies, Brokers, and Independent Agents

1. Penalties for Non-compliance
2. FINTRAC Interpretation Notices
3. Compliance Questionnaire

Reporting

1. **Suspicious transactions**

   You must report where there are reasonable grounds to suspect that a transaction or an attempted transaction is related to the commission or attempted commission of a money laundering offence or a terrorist activity financing offence.

   See Guideline 2*: Suspicious Transactions* and Guideline 3*: Submitting Suspicious Transaction Reports to FINTRAC*

2. **Terrorist property**

   You must report where you know that there is property in your possession or control that is owned or controlled by or on behalf of a terrorist or a terrorist group.

See Guideline 5*: Submitting Terrorist Property Reports to FINTRAC*

3. **Large cash transactions**
   You must report large cash transactions involving amounts of $10,000 or more received in cash.

   See Guideline 7*: Submitting Large Cash Transaction Reports to FINTRAC*

Record Keeping

You must keep the following records:

1. Large cash transaction records
2. Client information records
3. Copies of official corporate records (binding provisions)
4. Copies of suspicious transaction reports
5. Beneficial ownership records

See Guideline 6A*: Record Keeping and Client Identification for Life Insurance Companies, Brokers, and Agents*

Ascertaining Identity

You must take specific measures to identify the following individuals or entities:

1. Any individual who conducts a large cash transaction
2. Any individual or entity that purchases an annuity or life insurance policy for which it may pay $10,000 or more (including reasonable measures to obtain beneficial ownership information for an entity)
3. Any individual for whom you have to send a suspicious transaction report (reasonable measures and exceptions apply)
4. Any individual member of a group plan account when contributions to the plan are not made by payroll deductions or by the plan's sponsor

See Guideline 6A*: Record Keeping and Client Identification for Life Insurance Companies, Brokers, and Agents*

Politically Exposed Foreign Person

If you receive a lump-sum payment of $100,000 from an individual for an annuity or a life insurance policy, you have to take reasonable measures to determine whether you are dealing with a politically exposed foreign person. You also have to keep records and take additional measures.

See Guideline 6A*: Record Keeping and Client Identification for Life Insurance Companies, Brokers, and Agents*

Third Party Determination

Where a large cash transaction record is required, you must take reasonable measures to determine whether the individual is acting on behalf of a third party. In addition, where an annuity or life insurance policy is purchased and the client is required to pay $10,000 or more over the duration of the policy, you must take reasonable measures to determine whether the client is acting on behalf of a third party.

In cases where a third party is involved, you must obtain specific information about the third party and their relationship with the individual providing the cash or the client.

See Guideline 6A*: Record Keeping and Client Identification for Life Insurance Companies, Brokers, and Agents*

Compliance Regime

The following five elements must be included in a compliance regime:

1. The appointment of a compliance officer
2. The development and application of written compliance policies and procedures
3. The assessment and documentation of risks of money laundering and terrorist financing, and measures to mitigate high risks
4. Implementation and documentation of an ongoing compliance training program
5. A documented review of the effectiveness of policies and procedures, training program and risk assessment

See Guideline 4*: Implementation of a Compliance Regime*

Penalties for Non-compliance

Non-compliance with Part 1 of the *Proceeds of Crime (Money Laundering) Terrorist Financing Act* may result in criminal or administrative penalties.

Overview of Canada's Anti- Spam Legislation

Canada's Anti-Spam Legislation ("CASL") came into force on July 1st, 2014. After that date, organizations will either have to have the prior consent of intended recipients of commercial electronic messages, or ensure that the messages being sent, or the recipients of those messages, are exempt from the requirements to get consent. Some technology-related provisions of CASL are deferred until 2015, with private rights of action only becoming available starting in 2017.

The legislation, passed in 2010 and fully entitled "An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act", is designed to deter the most dangerous forms of spam in Canada.
However, CASL will impact all organizations due to the broad scope of the regulatory program it introduces.

The full text of CASL and its regulations can be found **here** on the Industry Canada website.

WHAT'S COVERED?

Commercial electronic messages (CEM), essentially, email. All email. The scope of CASL is far-reaching with significant implications for entities carrying on business in Canada and foreign entities that send CEMs into Canada. Malware, spyware, pretexting and the harvesting of electronic address and personal information will also be regulated under CASL.

THE GENERAL PROHIBITION – DON'T SEND UNSOLICITED CEMS

Under CASL, it is prohibited to send or cause or permit to be sent to an electronic address a commercial electronic message unless (a) the person to whom the message is sent has consented to receiving it, whether the consent is express or implied; and (b) the message complies with prescribed form and content requirements.

GENERAL REQUIREMENT – CONTENT OF MESSAGES

CASL requires a CEM to be in a form that must: (a) set out prescribed information that identifies the person who sent the message and the person — if different — on whose behalf it is sent; (b) set out information enabling the recipient to readily contact one of the persons referred to in paragraph (a); and (c) set out an unsubscribe mechanism complying with CASL standards. Organizations will want to undertake a review of the content of all their CEMs to ensure they comply with these provisions. Existing unsubscribe mechanisms may not meet the new standards set out in the CASL. In addition, there is a duty to ensure that the contact information about the sender remains valid for at least 60 days.

EXCEPTIONS

Having cast a broad net of prohibition, CASL provides some relief by designating certain exceptions. Firstly, the consent requirement does not apply to a CEM sent in a personal or family relationship or sent as an inquiry relating to the recipient's own commercial activity. In addition, the consent requirement does not apply to CEMs that solely:

a) provide requested product/service quotes;

b) further or complete an ongoing commercial transaction previously agreed to;

c) provide product warranty, recall, upgrade or similar information;

d) deal with ongoing subscriptions, memberships or similar relationships; or

e) concern an existing employment relationship.

The Regulations under CASL also exclude CEMs from all provisions of CASL if:

- they are sent within an organization;
- they are sent between organizations that already have a relationship, if the message concerns the activities of the organization to which the message was sent;
- they are sent on platforms where identification and unsubscribe information is conspicuously published and readily available to users, and where duplication of an unsubscribe or identification message would be repetitious;
- they are sent and received within limited access secure and confidential accounts (such as messages which a bank might send to an account holder);
- they are sent in response to a complaint, inquiry or request;
- they are sent on behalf of registered charities or political parties for fundraising purposes.

CASL also prescribes rules permitting certain first-time contact by email to referral prospects, but only if the detailed CASL rules are followed.

OTHER PROHIBITIONS

CASL also regulates the alteration of certain transmission data relating to a CEM, and prohibits the installation of computer programs such as cookies on recipient computers. Again, a prescribed form of consent would be needed, and certain exceptions are prescribed.

CONSENT

As noted above, with consent, CEMs can be sent. CASL sets out guidelines for obtaining consent, either express or implied. Consent can be oral, but a record of the consent needs to be retained. A person seeking consent must provide to the recipient certain information regarding the purpose for which consent is sought.

Further, prescribed information identifying the person seeking consent must be disclosed to recipients. Therefore, consents previously obtained and relied on to populate existing email databases might not continue to be valid.

Organizations will have to ensure on an ongoing basis that the purposes for which consent was originally obtained continue to apply to the substance of all the CEMs subsequently sent. This may limit the ability to use database lists in the future for a secondary use, and when subsequently modifying CEMs a check-back may be required to the scope of the initial consent obtained. CASL also contains some fairly complex rules if the intent is to have consent be available to future unknown third parties who may conduct co-marketing or similar arrangements.

Consent will be implied in certain circumstances, for:

a) "existing business relationships", as defined;

b) "existing non-business relationships", as defined;

c) certain circumstances where the email address of the recipient was made publicly available or voluntarily provided.

Commercial organizations will need to focus on the definition of "existing business relationship" set out in

CASL. That definition relies on relationships which are "current", defined as being within the past two years

(or an inquiry or application made in the last six months). As a result, "stale" entries on customer mailing lists may need to be purged unless another exemption or consent provision can be relied on. The definition of "existing non-business relationship" deals with memberships, volunteers, and donations. It establishes a similar two-year purge rule.

TRANSITION PERIOD

For existing relationships involving CEMs, CASL will provide for a three-year transition period under which consent can continue to be implied (unless expressly revoked).

Frequently Asked Questions About Canada's Anti-Spam Legislation

Does the legislation prohibit me from sending marketing messages?

No. Rather, it sets out some requirements for sending a certain type of message, called a commercial electronic message (CEM), to an electronic address. If you are sending a CEM to an electronic address, then you need to comply with three requirements. You need to: (1) obtain consent, (2) provide identification information, and (3) provide an unsubscribe mechanism.

What is a commercial electronic message?

A key question to ask yourself is the following: Is the message I am sending a CEM? Is one of the purposes to encourage the recipient to participate in commercial activity?

When determining whether a purpose is to encourage participation in commercial activity, some parts of the message to look at are: the content of the message

any hyperlinks in the message to website content or a database, and
contact information in the message.

These parts of the message are not determinative. For example, the simple inclusion of a logo, a hyperlink or contact information in an email signature does not necessarily make an email a CEM. Conversely, a tagline in a message that promotes a product or service that encourages the recipient to purchase that product or service would make the message a CEM.

Some examples of CEMs include:
offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land;
offers to provide a business, investment or gaming opportunity;
promoting a person, including the public image of a person, as being a person who does anything referred to above, or who intends to do so.

Does section 6 of CASL apply to commercial electronic messages (CEMs) sent between persons within an organization or sent between organizations?

No, there is an exemption for persons sending CEMs to other persons within their organization, where the CEMs concern the activities of the organization. Similarly, there is an exemption for persons sending CEMs to persons at another organization, where the CEMs concern the activities of that other organization and the organizations have a relationship. If the CEM does not concern the activities of the organization, or if the organizations do not have a relationship, then the requirements under section 6 of the legislation apply.

Consent
There are three general requirements for sending the CEM to an electronic address. You need (1) consent, (2) identification information and (3) an unsubscribe mechanism. The questions under this

heading relate to the first requirement, namely consent. There are two types of consent under CASL – express and implied. How can I obtain express consent?

Consent can be obtained either in writing or orally. In either case, the onus is on the person who is sending the message to prove they have obtained consent to send the message.

The CRTC has issued information bulletins to provide guidance and examples of recommended or best practices. Compliance and Enforcement Information Bulletin CRTC 2012-548, among other things, helps explain what information is to be included in a request for consent. The Bulletin also suggests some key considerations that may make tracking or recording consent easier, and therefore, may make it easier to prove consent. They are: whether consent was obtained in writing or orally when it was obtained, why it was obtained, and the manner in which it was obtained.

Do I need consent to send a commercial electronic message following a referral?

There is an exception to the consent requirement for commercial electronic messages (CEMs) sent following a referral if certain conditions are met. The referral must be made by an individual who has an existing business relationship, an existing non-business relationship, a family relationship or a personal relationship with the sender and the recipient of the CEM. Also, the full name of the individual who made the referral and a statement that the CEM is sent as a result of a referral must be in the CEM.

The CEM must still respect the other two requirements – it must contain the identification information, and an unsubscribe mechanism.

Someone gives me a business card: Is that clear consent to add them to my distribution list?

You may have their implied consent to send them CEMs, as long as:

the message relates to the recipient's role, functions or duties in an official or business capacity; and the recipient has not made a statement when handing you the business card that they do not wish to receive promotional or marketing messages (CEMs) at that address.

It is important to remember that the onus is on the sender to prove they received consent.

Recall that consent under CASL is also implied if you have an existing business relationship, existing nonbusiness relationship with the person.

Compliance will be examined on a case-by-case basis in light of the specific circumstances of a given situation.

The National DNCL Rules

What are the National DNCL Rules?

The National DNCL Rules are a subset of the CRTC's Unsolicited Telecommunications Rules. The Rules require that telemarketers who call on their own behalf and financial agencies and advisors who engage a third party to call on their behalf (client of a telemarketer) subscribe to, pay fees for, and access the National DNCL. The National DNCL Rules prohibit telemarketers and clients of telemarketers from calling telephone numbers that have been registered on the National DNCL for more than 31 days. All telemarketers and clients of telemarketers must follow these Rules unless they are making calls that are specifically exempted from the National DNCL Rules.

What are the Unsolicited Telecommunications Rules?

The Unsolicited Telecommunications Rules include the Telemarketing Rules, the Automatic Dialing-Announcing Device (ADAD) Rules and the National DNCL Rules. All telemarketers and clients of telemarketers must follow the Telemarketing Rules and the ADAD Rules regardless of whether they are making calls that are specifically exempted from the National DNCL Rules. The full set of Rules can be found on the Telemarketing information page in the Consumers section of the CRTC website. You can also read a condensed version of the Rules in the National Do Not Call List and Telemarketing Rules.

What are the definitions of terms used in the National DNCL Rules.

Telemarketing: Telemarketing is the use of telecommunications facilities to make telephone calls or send faxes to consumers for the purpose of solicitation. Solicitation covers a wide range of activities, including sales calls, prospecting calls, and calls for charitable donations or volunteers. Any organization has the potential to be a telemarketer.

Solicitation: Solicitation is the act of selling or promoting a product or service – or requesting money or "money's worth" – directly or indirectly, for oneself or another party.

Telemarketer: If you make telemarketing calls or send telemarketing faxes on your behalf or behalf of one or more other businesses (i.e. clients), then you are a telemarketer.

A client of a telemarketer: If you engage a third party to make telemarketing calls or send telemarketing faxes on your behalf, then you are a client of a telemarketer. The third party must also comply with Unsolicited Telecommunications Rules.

Scrubbing: This is an industry term that describes removing telephone numbers on the National DNCL from a telemarketer's calling lists.

Express consent: This is permission given by a consumer to a telemarketer for receiving telemarketing calls from that telemarketer and for receiving telemarketing calls via an ADAD.

Are all unsolicited calls considered to be telemarketing calls?

No, not all unsolicited calls are telemarketing calls. Calls that are ***not*** considered telemarketing calls, and do ***not*** need to follow the National DNCL Rules but may need to follow the ADAD Rules include:

1. Product recall calls
2. Appointment reminder calls
3. Appointment rescheduling calls
4. Calls related to payment or bill collections
5. Public service announcements
6. Calls for market research, surveys or public opinion polls

Do the Rules extend to telemarketers from outside of Canada?

Yes. The Rules apply regardless of where the call originates. Telemarketers calling Canadian consumers from outside of Canada must comply with the National Do Not Call List Rules.

Exemptions to the National DNCL Rules

Do all telemarketing calls fall under the National DNCL Rules?

No, some types of telemarketing calls are exempt.

These types of telemarketing calls are exempt from the National DNCL Rules:

1. Calls made by or on behalf of:
    1. Canadian registered charities
    2. political parties, riding associations, and candidates
    3. newspapers of general circulation for the purpose of soliciting subscriptions

2. Calls made to:
    1. Consumers with whom you have an existing business relationship
    2. Consumers who have provided express consent for receiving telemarketing calls
    3. Business Consumers

National Do Not Call List Exemptions

Telemarketers should understand that there are certain kinds of telemarketing calls that are exempt from the National DNCL Rules.

The exemptions include telemarketing calls made by, or on behalf of:

1. Canadian registered charities;
2. Political parties, riding associations and candidates; and
3. Newspapers of general circulation for the purpose of soliciting subscriptions.

Telemarketing calls that are made to persons with whom there is an existing business relationship are also exempt. Telemarketers are free to call a consumer who:

1. Has purchased, leased, or rented a product or service from the telemarketer in the last 18 months;
2. Is in possession of a written contract with a telemarketer for a service that is still in effect or expired within the last 18 months; and/or
3. Has made an inquiry or has submitted an application to a telemarketer about a product or service within the last 6 months.

Telemarketers may also make calls to consumers if the consumer has provided express consent to be called. Express consent includes:

1. The consumer's permission to be called on a written form, electronic form, or an online form; or
2. The consumer's verbal permission.

The National DNCL Rules do not apply to telemarketing calls made to businesses

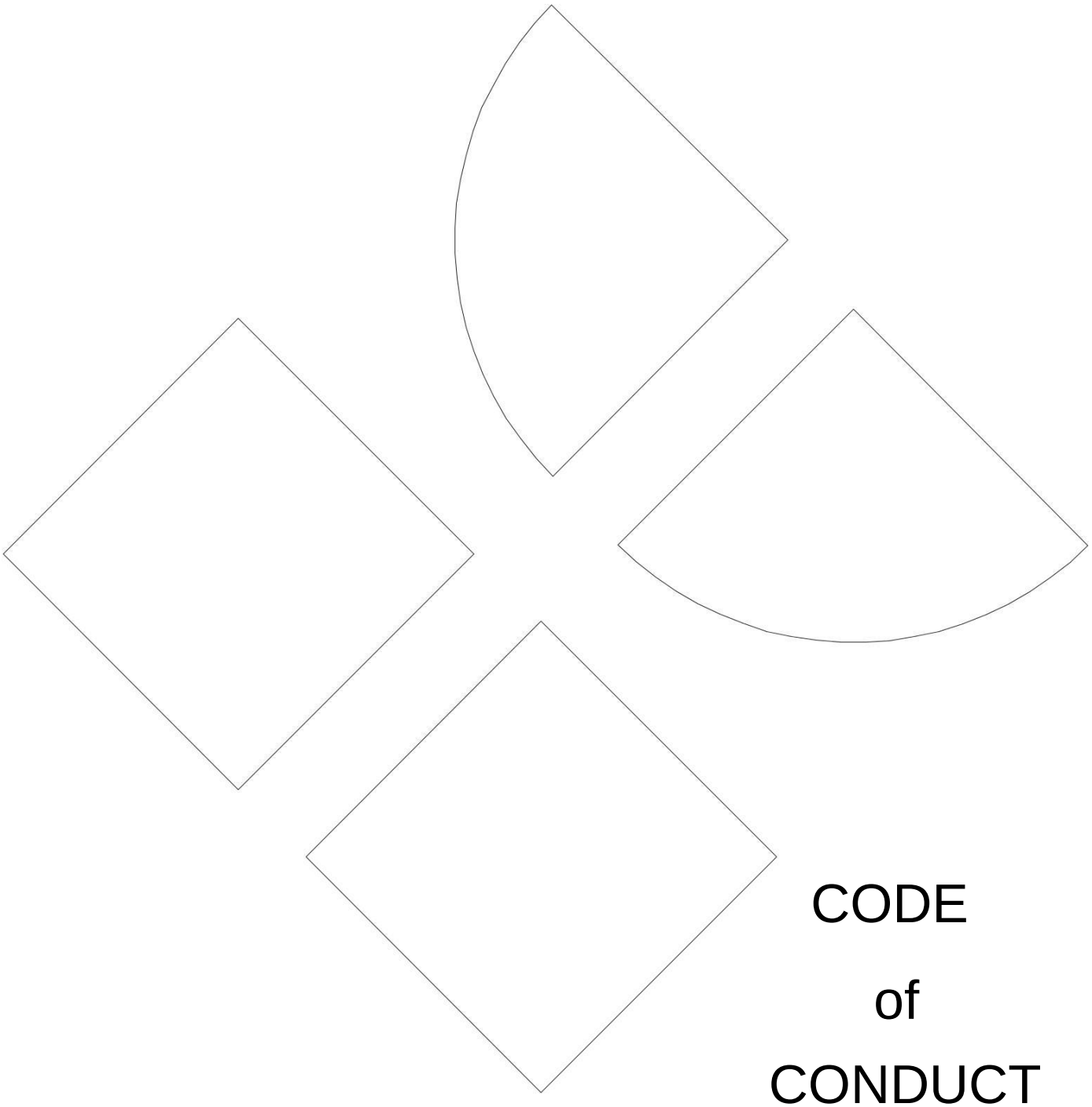
Appendix

1. Insurance Council of BC Code of Conduct

2. Manulife Code of Conduct

3. Remarks by Jeanne M. Flemming, Director, FINTRAC

INSURANCE COUNCIL OF BRITISH COLUMBIA



CODE of CONDUCT

IMPORTANT INFORMATION REGARDING THE CONTENTS OF THIS CODE

Unless otherwise qualified in this Code, read:

- "Act" as the *Financial Institutions Act*;
- "adjusting firm" as a licensed corporation or partnership, or an individual sole proprietor insurance adjuster, that meets the nominee requirements set out in Council Rules;
- "agency" as a licensed corporation or partnership, or an individual sole proprietor agent, that meets the nominee requirements set out in Council Rules;
- "client" as a person who may reasonably be expected to rely on a licensee's advice or actions in relation to insurance;
- "Code" as the Code of Conduct;
- "Council" as the Insurance Council of British Columbia;
- "licensee" as a licensed insurance salesperson, agent or adjuster;
- "nominee" as a licensee nominated to exercise the rights and privileges of an insurance licence issued to an insurance agency or an insurance adjusting firm;
- "principal" as a person on whose behalf a licensee has undertaken to perform adjusting services;
- "person" includes a corporation, partnership, society, association or other organization or legal entity;
- "Rule" as a rule made by Council pursuant to section 225.1 of the Act; and
- "transaction" as a situation in which a licensee provides an insurance product or service to any person.

Suite 300 - 1040 West Georgia Street

Vancouver, BC V6E 4H1

Telephone: 604-688-0321 Within BC: 1-877-688-0321 Fax: 604-662-7767

insurancecouncilofbc.com

TABLE OF CONTENTS

1. INTRODUCTION

The strength of the insurance industry is based, in part, on industry members providing advice and services to the public in a competent and professional manner. The underlying principle of all insurance business is utmost good faith. To command the confidence and respect of the public, the insurance industry must maintain a reputation for integrity, competence, and good faith.

The provincial legislature has entrusted Council with the responsibility for maintaining standards of professional conduct in the insurance industry. The Act and Rules empower Council to set standards for insurance salespersons, agents and adjusters and to take remedial action where those standards have not been met. Rule 7(8) requires that licensees comply with this Code.

Council's mission statement is:

We serve the public by ensuring

licensed insurance agents, salespersons and adjusters act within a professional framework,

which promotes ethical conduct, integrity, and competence.

In keeping with Council's mandate, the purpose of the Code is to define and communicate standards of conduct for use by licensees in their practice of the business of insurance. The Code is also used as a guide by Council in its deliberations on proper and usual practice in particular circumstances.

The Code sets out minimum standards of conduct. The extent to which each licensee rises above these standards is a personal decision. However, by striving to maintain the highest possible standards of ethical conduct, a licensee will enjoy the respect and confidence of the public and other members of the industry.

Licensees have a responsibility to assist in the regulatory process and act as gatekeepers for the industry by discouraging misconduct and reporting it where identified.

2. INTERPRETATION

The Code is divided into a number of subsections, each of which addresses a specific principle. Each Principle is defined and then further clarified with a stated Requirement. To provide licensees with additional guidance, each subsection also includes Guidelines and Examples of Misconduct taken from past Council decisions.

The Code provides a framework for a licensee to measure his or her conduct in particular circumstances. It is not possible to foresee every possible situation and describe the proper conduct. When reading the Code, keep in mind that although presented separately, all principles and requirements are interconnected. For example, the principle of Trustworthiness is fundamental to all activities of a licensee and to each of the principles outlined.

The Code applies to all licensees and should be read and interpreted in the context of a licensee's area of insurance practice and Council's primary concern, which is protection of the public interest. For clarity the Code refers to licensees by the first person "you".

The Code is written in plain language to be clear and concise and should be read in conjunction with governing legislation and the Rules. Council has additional resources available which expand on many of the principles and requirements detailed in the Code. These include our Notices and Bulletins which are available on our website at insurancecouncilofbc.com, as well as appendixes to the Code. Throughout the Code, when a published article or appendix was identified as addressing a particular subject, the Notice, Bulletin, or appendix is referenced.

3. TRUSTWORTHINESS

3.1 PRINCIPLE

In an industry where trust is the foundation for all dealings, you must meet rigorous standards of personal integrity and professional competence. These characteristics speak to the essence of what a licensee does. Failure to adhere to these standards reflects not only on you, but also on the profession. Trustworthiness is a fundamental element of each requirement in the Code.

3.2 REQUIREMENT

You must be trustworthy, conducting all professional activities with integrity, reliability and honesty. The principle of trustworthiness extends beyond insurance business activities. Your conduct in other areas may reflect on your trustworthiness and call into question your suitability to hold an insurance licence.

3.3 GUIDELINES

3.3.1 Conduct that would reflect adversely on your trustworthiness includes:

a) dishonestly dealing with money or property;
b) improper use of your position or knowledge as a licensee for personal benefit; (Bulletin - April 2003)
c) intentionally misleading clients, insurers or Council through false statements or by withholding material information;
d) knowingly prejudicing the interests of a client or principal for personal gain; and
e) conduct in the nature of theft or fraud.

3.3.2 Acts of dishonesty outside your professional life may reflect on your trustworthiness to hold an insurance licence.

3.4 EXAMPLES OF MISCONDUCT

3.4.1 A chartered accountant accepted unsecured loans from clients, breached terms of a suspension order, swore a false affidavit and mishandled trust funds.

3.4.2 While acting in a position of trust for a volunteer organization, misappropriated funds from the organization.

3.4.3 Used confidential client information provided by an insurer for a purpose other than intended. (Appendix B)

3.4 Examples Of Misconduct - continued

3.4.4 Made or assisted in making a false insurance claim.

3.4.5 Materially misrepresented odometer readings and previous vehicle damage in the private sale and registration of a licensee's motor vehicles.

3.4.6 Signed and submitted segregated fund applications solicited and completed by another agent, to help the other agent circumvent the insurer's internal policy that prohibited life agents from selling segregated funds unless they were also licensed to sell mutual funds.

3.4.7 Improperly rated a motor vehicle to circumvent AirCare.

3.4.8 Made false declarations to an insurer.

3.4.9 "Witnessed" a signature known to be a forgery.

3.4.10 Made false or misleading statements to Council.

3.4.11 Raised capital from clients of an insurance agency of which the licensee was owner and principal, without disclosing to the clients that they were investing in the agency and without providing material information to them about the investment, such as agency financial statements and disclosure on how the investments would be used.

4. GOOD FAITH

4.1 PRINCIPLE

The insurance industry is based on fiduciary relationships. Accordingly, the exercise of good faith by licensees in the practice of the business of insurance is essential to public confidence in the industry. Good faith is a fundamental aspect of your conduct and a key element in each of the Code's requirements.

4.2 REQUIREMENT

You must carry on the business of insurance in good faith. Good faith is honesty and decency of purpose and a sincere intention on your part to act in a manner which is consistent with your client's or principal's best interests, remaining faithful to your duties and obligations as an insurance licensee.

You also owe a duty of good faith to insurers, insureds, fellow licensees, regulatory bodies and the public.

4.3 GUIDELINES

4.3.1 Conduct that would reflect adversely on your intention to practice in good faith includes:

a) wilful disregard of duties and obligations under the Act, Rules and Code;
b) misrepresentation or failure to disclose material information where required; (Bulletin - November 2002)
c) unauthorized access, use or disclosure of confidential information; (Appendix B)
d) making improper use of your position as a salesperson, agent or adjuster;
e) employing or remunerating unlicensed persons to conduct insurance business; and
f) taking advantage of a client's or insured's inexperience, ill health or lack of sophistication.

4.4 EXAMPLES OF MISCONDUCT

4.4.1 Signed as witness to applications, but had not in fact seen them signed.

4.4.2 Directed an employee to sign a document as agent of record, when the employee had not completed the form or met the policyowner.

4.4.3 Directed an unlicensed employee to take an insurance application.

4.4.4 Submitted applications that were known to have been completed by an unlicensed person.

4.4 Examples of Misconduct - continued

4.4.5 Used premium money for personal use.

4.4.6 Backdated a client's automobile insurance and subsequently lied to an ICBC adjuster about when and how the transaction was processed.

4.4.7 Counseled a client to misrepresent material information to an insurance company.

4.4.8 Accessed confidential client information from an insurer's computer database without authority and subsequently communicated that information to another person. (Appendix B)

4.4.9 Drafted and signed a false certificate of insurance for a family member who required evidence of insurance coverage.

5. COMPETENCE

5.1 PRINCIPLE

Clients rely on the knowledge and advice of licensees. Accordingly, competence on the part of licensees is an essential requirement of the practice of the business of insurance. Incompetent conduct can result in significant prejudice to clients and insurers. It follows that you should not undertake to perform any insurance services beyond your level of competence.

5.2 REQUIREMENT

You must conduct all insurance activities in a competent manner. Competent conduct is characterized by the application of knowledge and skill in a manner consistent with the usual practice of the business of insurance in the circumstances.

You must continue your education in insurance to remain current in your skills and knowledge.

5.3 GUIDELINES

5.3.1 Your practice and level of service to clients should be consistent with that which a reasonable and prudent licensee in similar circumstances would exercise. Honest mistakes do not necessarily constitute a failure to adhere to the Code.

5.3.2 Conduct that would reflect on your competence includes:

a) failing to properly place insurance coverage as instructed;
b) failing to provide evidence of insurance coverage when required;
c) failing to advise a client of a lapse or change in insurance coverage;
d) failing to conduct an adequate fact finding and assessment of a client's insurance needs;
e) failing to properly handle and account for money or property;
f) failing to maintain proper and adequate books and records of insurance transactions and related financial affairs;
g) failing to provide for the safekeeping and confidentiality of records (Appendix B);
h) failing to advise an insurer/principal of a risk or claim;
i) failing to properly document communications and instructions from a client to ensure mutual understanding and provide a record of the transaction; and
j) practicing in an area where you lack sufficient expertise, training or experience.

5.3.3 Nominees are responsible to Council for all activities of the insurance agency or adjusting firm and must ensure the agency or firm and its employees are properly supervised and operate in accordance with the conditions and restrictions on their licences.

5.3 Guidelines - continued

5.3.4 Licensees who have supervisory duties must fulfil those duties competently. Improper practice by supervised employees may bring a supervisor's competence into question if the conduct occurred due to inadequate supervision, including lack of policies, procedures and training.

5.3.5 You must comply with the continuing education requirements under the Rules. However, these are minimum requirements and may not be sufficient to maintain appropriate standards, particularly if you work in specialized areas.

5.3.6 You must refrain from giving advice in areas beyond your expertise as an insurance licensee. For example, you should refer matters that would be more properly dealt with by a lawyer or accountant.

5.4 EXAMPLES OF MISCONDUCT

5.4.1 Sold an insurance policy that was inappropriate given the client's stated objectives and circumstances and that a prudent and competent agent would not have recommended.

5.4.2 Counseled a client to conduct an assignment of a life insurance policy in a manner that failed to meet the client's stated objective.

5.4.3 Failed to properly manage the business and financial aspects of an agency, including the proper handling and remittance of premium money to insurers.

5.4.4 Altered the effective date of an insurance contract.

5.4.5 Permitted a Level 1 salesperson to conduct general insurance business without the direct supervision of a Level 2 or Level 3 agent.

5.4.6 Employed an unlicensed individual in a licensed capacity for a period of five months because procedures were inadequate to ensure employees were properly licensed before they commenced insurance activities.

5.4.7 Provided written notice to clients that their insurance coverage had been renewed, prior to receiving confirmation from the insurance company that renewal terms would be offered.

6. FINANCIAL RELIABILITY

6.1 PRINCIPLE

As an insurance licensee, clients and insurers entrust money, property and financial instruments to you to facilitate transactions or claims on their behalf. Accordingly, your reliability in handling these funds is essential to your practice as a licensee.

6.2 REQUIREMENT

You must be financially reliable. This means you can be relied upon to properly safeguard and account for money and property entrusted to you and to promptly deliver them in accordance with the circumstances.

6.3 GUIDELINES

6.3.1 Conduct outside your professional life may reflect on your financial reliability.

6.3.2 Outstanding judgements, pending legal proceedings and/or bankruptcies can reflect on your financial reliability.

6.3.3 Where you collect or receive funds on behalf of an insurer, you must:

a) not encumber the funds without the prior written consent of the insurer;
b) not use or apply the funds for purposes other than as described in the agreement with the insurer; and
c) pay to the insurer all funds collected or received less any deductions authorized by the insurer.

6.4 EXAMPLES OF MISCONDUCT

6.4.1 Failed to account for or repay unauthorized withdrawals from a bank account over which the licensee held a power of attorney.

6.4.2 Failed to invest a client's money in mutual funds as instructed.

6.4.3 Contrary to his clients' interests and for personal gain, solicited clients to invest the cash value of their life insurance policies in a company he had a vested interest in, without disclosing his inherent conflict of interest and the true risks involved.

6.4.4 Personal debts and questionable financial involvement with a number of companies that solicited investors for offshore investments.

6.4.5 Legal proceedings by a group of former clients alleging misappropriation of funds and by a bank seeking payment for personal credit line agreements and two promissory notes.

7. USUAL PRACTICE: DEALING WITH CLIENTS

7.1 PRINCIPLE

Under the Code, a client includes anyone who might reasonably be expected, in the circumstances, to rely on your professional advice or actions in relation to his or her insurance. You are required to put the best interests of the client as your first concern, as befits the role of a fiduciary.

7.2 REQUIREMENT

When dealing with clients you must:

- protect clients' interests and privacy;
- evaluate clients' needs;
- disclose all material information; and
- act with integrity, competence and the utmost good faith.

7.3 GUIDELINES

CONFLICT OF INTEREST

A conflict of interest exists when your loyalty to, or representation of, a client or insurance company could be materially or adversely affected by your interest or duty to another party. A conflict of interest may be real, potential or apparent.

Conflict of Interest of Guidelines for Insurance Agents, Adjusters, and Salespersons is included as Appendix A.

DISCLOSURE

7.3.1 What information is material and should be provided to a client depends on the circumstances of the transaction. You should disclose any information relevant to the client's insurance needs that a reasonable and prudent licensee would disclose in the same circumstances.

7.3.2 Prior to arranging an insurance transaction with a client who has been referred to you by an unlicensed third party, you must disclose to the client, in writing, any fee or compensation paid to the third party for the referral.

7.3 Guidelines - continued

7.3.3 Prior to conducting a transaction, you must disclose any fees you charge in addition to the policy premium. The fee should be disclosed in writing to the client and include separate dollar values for the total insurance premium charged by the insurer, the total additional fee charged by the agent and any premium finance fees charged by the agent.
(Bulletin - October 2001)

7.3.4 You must disclose to the client any arrangement to place the client's insurance through another agent and meet Council's sub-brokering guidelines.
(Notice ICN# 98-003 - Sub-Brokering)

7.3.5 You must fully inform clients about all aspects of the insurance products they purchase, including any changes that occur during the term of the policy.

7.3.6 You must make full and fair disclosure of all material facts to enable clients to make informed decisions regarding their insurance.

7.3.7 You must not use sales materials or illustrations that are misleading or unnecessarily confusing.

7.3.8 You must not use terms such as "guaranteed" without appropriate qualification or evidence to support the statement.

DUTY OF CARE

7.3.9 The client's interests take priority over your interests and should not be sacrificed to the interests of others. You must not engage in practices that place the interests of others ahead of the client's interests.

CONFIDENTIALITY

7.3.10 You must hold in strict confidence all information acquired in the course of your professional relationship concerning the personal and business affairs of a client, and must not divulge or use such information other than for the purpose of that transaction or of a similar subsequent transaction between you and the same client unless expressly authorized by the client or as required by law. (Appendix B)

7.3.11 If you choose to terminate your business relationship with a client you must do so in a manner that avoids prejudice and allows for the orderly transfer of the client's insurance business elsewhere. You must provide the client with adequate notice of your intent to withdraw your services, as well as comply with any applicable statutory and professional obligations.

7.3.12 Clients should be notified at least 30 days prior to the expiration of their existing insurance if you are unable to renew their insurance at the same terms and conditions. (Notice ICN# 03-004 - Brokering in a Difficult Market)

7.3 Guidelines - continued

PROTECTING CLIENTS' INTERESTS

7.3.13 You must report all claims promptly.

7.3.14 You must deliver insurance policies or evidence of insurance coverage within a reasonable time and, in any event, in accordance with the terms of your agreement with the insurance company.

7.3.15 You must deal with all formal and informal complaints or disputes in good faith and in a timely and forthright manner, including, when necessary, referring the complainant to other more appropriate people, processes and/or organizations.

7.4 EXAMPLES OF MISCONDUCT

7.4.1 Failed to fully assess a client's needs and objectives and neglected to advise the client of changes to the insurance plan as a consequence of a medical rating.

7.4.2 Provided a copy of a client's insurance policy to two other customers as an example of the product being offered. (Appendix B)

7.4.3 Failed to refund all money due to a client in accordance with the cancellation provisions set out in the client's insurance contract and as agreed to in the licensee's contract with the insurer.

7.4.4 Requested an insurer cancel a client's insurance policy for non-payment of premium, when the premium had been paid, in order to apply the pro-rata return premium against an outstanding debt owed by the client.

8. USUAL PRACTICE: DEALING WITH INSURERS

8.1 PRINCIPLE

Licensees act as intermediaries between clients, insureds and insurers in a contractual relationship. The insurers' ability to meet their contractual duties is based on your honesty and competence in providing advice and information.

8.2 REQUIREMENT

You have a duty to insurers with whom you are transacting business to:

- make reasonable inquiries into the risk;
- provide full and accurate information;
- promptly deliver all insurance documents and monies due;
- represent the insurer's products fairly and accurately;
- adhere to the authority granted by the insurer; and
- promptly report all potential claims.

You must not defame or discredit insurers.

8.3 GUIDELINES

CONFLICT OF INTEREST

A conflict of interest exists when your loyalty to, or representation of, a client or insurance company could be materially or adversely affected by your interest or duty to another party. You have a responsibility to avoid a conflict of interest with an insurer. A conflict of interest may be real, potential or apparent.

Council's *Conflict of Interest of Guidelines for Insurance Agents, Adjusters, and Salespersons* is included as Appendix A.

DISCLOSURE

8.3.1 You have a duty to fully and accurately disclose any information material to the insurer's decision to issue a contract of insurance.

8.3.2 Where you are placing insurance on behalf of another agent who is acting for the insured, you should disclose this to the insurer.

DUTY OF CARE

Insurers rely on licensees for information to make underwriting decisions. Therefore, you must make reasonable inquiries into a risk. This means making inquiries that a reasonable and prudent licensee would make in the same circumstances.

8.3.3 In accordance with the Rules, it is a condition of every licence issued that, where the licensee collects or receives insurance premiums on behalf of an insurer, the licensee must:

a) not encumber the funds without the prior written consent of the insurer;
b) not use or apply the funds for purposes other than as described in the agreement with the insurer; and
c) pay to the insurer all funds collected or received less any deductions authorized by the insurer.

8.3.4 Insurance should be sold or conserved based on the merits of the particular policy as it relates to the needs of the client. Attempts to discredit insurance companies are not the proper practice of the business of insurance. This requirement is not meant to prevent licensees from providing information that is relevant to the client's ability to make an informed decision about his or her insurance. However, information offered solely for the purpose of undermining the reputation of an insurer is inappropriate.

8.4 EXAMPLES OF MISCONDUCT

8.4.1 Failed to remit to the insurer all premiums collected or received in accordance with the terms of the agency's agreement with the insurer.

8.4.2 Offered and bound terms under a policy that were not authorized by the insurer.

8.4.3 Issued a cover note purporting to bind an insurer the agency did not represent

9. USUAL PRACTICE: DEALING WITH LICENSEES

9.1 PRINCIPLE

Along with your fellow licensees, you represent the insurance industry to the public. The public views the industry as a single entity, so by maligning a fellow licensee you are bringing your own reputation and that of the industry into public disrepute. Treating your colleagues with courtesy and respect enhances your own reputation and the public's confidence in the insurance industry

9.2 REQUIREMENT

You must not defame or discredit other licensees.

9.3 GUIDELINES

9.3.1 Insurance should be sold or conserved based on the merits of the particular policy as it relates to the needs of the client. Attempts to discredit another licensee are not the proper practice of the business of insurance. This rule is not meant to prevent licensees from providing information that is relevant to the client's ability to make an informed decision about his or her insurance. However, information offered solely for the purpose of undermining the reputation of another licensee is inappropriate.

9.4 EXAMPLE OF MISCONDUCT

9.4.1 Used the Discipline section of the Bulletin to discredit another licensee.

10. USUAL PRACTICE: DEALING WITH THE PUBLIC

10.1 PRINCIPLE

The insurance industry provides services upon which the well-being of individuals and businesses will often depend. Therefore, it is incumbent upon all licensees to take their duty of care to the public seriously. Your forthrightness and conduct in representing yourself and your services reflects on other licensees and the industry as a whole. Accordingly, it is in the interest of all licensees to conduct themselves in a manner that promotes public confidence in the integrity and reliability of the industry.

10.2 REQUIREMENT

You must honestly represent yourself and the services and products you provide so as not to mislead the public.

10.3 GUIDELINES

HOLDING OUT

10.3.1 You must hold yourself out in the manner in which you are licensed.

10.3.2 You must disclose you are an insurance agent prior to conducting insurance activities with the public.

10.3.3 You must not use the term “and Associates”, or similar phrase, as part of a business or trade name when there are not two or more licensees in the business.

10.3.4 You must not represent yourself as having specific expertise in a given area of practice or industry designations unless you are suitably qualified by virtue of your experience, training or both.

10.3.5 You must not purport to be a financial planner or provide financial planning advice, unless you meet the qualifications and disclosure requirements set by Council.
(Notice ICN# 02-001 - Financial Planning)

10.3.6 You must not make any false or misleading statements in the solicitation of or negotiation for insurance.

ADVERTISING

10.3.7 You must not engage in misleading advertising by offering prices, rates of return, products or services you cannot reasonably provide or that are subject to undisclosed qualifications.

11. USUAL PRACTICE: CONDUCT SPECIFIC TO INSURANCE ADJUSTERS

11.1 PRINCIPLE

Each requirement under the Code applies equally to all licensees. However, insurance adjusters play a unique role in the business of insurance, particularly in their relationships with insureds and insurers. Accordingly, the following sets out additional, specific duties applicable to licensees engaged in the role of insurance adjusting. This does not limit applicable duties under the other requirements of the Code. Adjusters must also refer to and comply with each requirement identified in the Code in the course of their practice.

11.2 REQUIREMENT

DUTIES TO PRINCIPALS

You must:

- protect your principal's interests;
- protect your principal's confidential information;
- disclose all information material to the loss or claim;
- decline to act where you have an undisclosed conflict of interest or financial interest in a loss or claim; and
- act within the authority and instructions of your principal.

DUTIES TO INSUREDS

You must:

- properly identify yourself, your principal and your role as an adjuster;
- adjust claims promptly and fairly;
- protect the insured's confidential information; and

- fully disclose information material to the insured's policy coverage, rights and obligations.

11.3 GUIDELINES

CONFLICT OF INTEREST

A conflict of interest exists when your loyalty to, or representation of, a client, insurance company, or principal could be materially or adversely affected by your interest or duty to another party. You have a responsibility to avoid a conflict of interest with an insurer. A conflict of interest may be real, potential, or apparent.

Council's *Conflict of Interest of Guidelines for Insurance Agents, Adjusters, and Salespersons* is included as Appendix A.

11.3 Guidelines - continued

11.3.1 You must take reasonable steps to keep the insured informed of the status of a claim and respond promptly to the insured's communications.

11.3.2 You must not attempt to influence a claim through coercion, false or misleading statements or other improper means.

11.3.3 You must not seek to discourage legitimate claims or cause undue delay in adjusting a claim.

11.3.4 You must fully and promptly inform insureds of material information regarding policy coverage, limitation periods, claim denials and their rights and obligations in the claims process, as required in the circumstances.

11.3.5 You must not mislead anyone as to your role in adjusting a claim. This includes who is your principal. For example, when acting on behalf of an insurance company, you should advise the insured in your first meeting that you act for the insurance company in the claim and that the insured is responsible for the hiring and work of contractors, even if facilitated by you.

11.3.6 You must refrain from giving legal advice or discouraging insureds from seeking legal advice.

11.3.7 You must not deal directly with an insured represented by legal counsel without consent.

11.3.8 You must only act on an adjustment when you have authority from your principal, and then according to your principal's instructions.

11.3.9 You must not obtain medical information about an individual without the consent of that person. (Appendix B)

11.4 EXAMPLES OF MISCONDUCT

11.4.1 Failed to identify a provision in a policy which required the insured to repair or replace damaged property within 180 days from the date of the loss in order to receive replacement cost.

11.4.2 Entered a restricted fire scene for the purpose of adjusting the property loss without authorization from the local fire department.

11.4.3 Disclosed confidential information in promotional material, including testimonials from claim files, claimant names, file numbers, negotiated settlements and liability decisions. (Appendix B)

12. DEALING WITH THE INSURANCE COUNCIL OF BRITISH COLUMBIA

12.1 PRINCIPLE

12.2

Licensees benefit from a degree of self- regulation under the Act, in that they are able to participate in the regulation of their industry. This privilege requires the co-operation and support of licensees.

12.2 REQUIREMENT

You must respond promptly and honestly to inquiries from Council.

12.3 GUIDELINES

12.3.1 Section 231(1)(d) of the Act requires licensees to make a prompt reply to an inquiry from Council.

12.3.2 It is a breach of the Act under section 231(1)(c) to make a material misstatement in an application for a licence or in response to an inquiry from Council.

12.4 EXAMPLES OF MISCONDUCT

12.4.1 Failed to reply over several months to a number of inquiries from Council during the course of a Council investigation.

12.4.2 Swore a false affidavit advising Council that insurance activities had not been conducted while unlicensed.

12.4.3 Provided false and misleading information on licensing applications to conceal not having sufficient credits to meet the continuing education licence condition.

12.4.4 Made material misstatements in reply to an inquiry from Council.

12.4.5 Refused to reply to an inquiry from Council.

13. COMPLIANCE WITH GOVERNING LEGISLATION AND COUNCIL RULES

13.1 PRINCIPLE

Licensees are expected to adhere to all regulatory requirements. In terms of professional practice, as a licensee you come under the direct regulation of the Financial Institutions Commission and Council. Violation of the regulatory requirements administered by these bodies not only contravenes the Code, it can also subject you to prescribed disciplinary action under the Act.

13.2 REQUIREMENT

You must be aware of and comply with your duties and obligations under the Act, the *Insurance Act*, the Rules and the Code.

13.3 GUIDELINES

13.3.1 You are required to read, understand and remain current on the applicable regulatory requirements that apply to you under the Act and Rules. This information is readily available from a variety of sources. As necessary, Council publishes guidelines and directives to licensees on specific issues through its Notices, Bulletins and website. To assist you, the following is a list of specific resources that should be particularly noted. Legislation is available online at bclaws.ca or at your local library. All other information is available on Council's website at insurancecouncilofbc.com or may be obtained by contacting Council's office.

13.3.2 You should also be aware of any other legislation, such as the *Income Tax Act, Motor Vehicle Act, or Personal Information Protection Act* which may impact your particular practice.

Publications

- *Financial Institutions Act*
- *Insurance Act*
- Council Rules
- Notices
- Bulletins
- Council Decisions
- Licence Conditions

CONFLICT OF INTEREST GUIDELINES

FOR INSURANCE AGENTS, ADJUSTERS, AND SALESPERSONS ("Giudelines")

Insurance agents, adjusters, and salespersons ("licensees") have a responsibility to avoid conflicts of interest arising between themselves and their clients or insurance companies. When a conflict of interest arises, or has the potential to arise, a licensee needs to take appropriate action before acting, or continuing to act, on behalf of a client, an insurance company, or other principal.

The purpose of these Guidelines is to identify situations, actions, or conduct that could lead to, or result in, a conflict of interest and to assist licensees in understanding the issues relating to conflicts of interest. In addition, these guidelines provide direction on how to plan for and address situations when a conflict of interest arises, which licensees may use to manage, or avoid, such conflicts. By doing so, it may reduce the risk of harm to all parties, including potential harm that could result to a licensee's reputation and insurance practice.

1. DEFINITION OF CONFLICT OF INTEREST

A conflict of interest exists when there is a risk that a licensee's loyalty to, or representation of, a client, an insurance company, or other principal could be materially or adversely affected by a licensee's own interests or by a licensee's duty to another client, former client, insurance company, or other third party.

Conflicts of interest include, but are not limited to:

a) A **real** conflict of interest denotes a situation in which a licensee has knowledge of a personal, private, financial, or professional interest that is sufficient to influence the exercise of his or her duties and responsibilities.

b) A **potential** conflict of interest incorporates the concept of foreseeability, such as when a licensee can foresee that a personal, private, financial, or professional interest may someday be sufficient to influence the exercise of his or her duties.

c) An **apparent or perceived** conflict of interest exists when a reasonable person has an apprehension that a conflict of interest exists. An apparent conflict of interest can exist where it could be perceived, or where it appears, that a licensee's

personal, private, financial, or professional interest or access to information could improperly influence the exercise of his or her duties, whether or not this is, in fact, the case.

Transparency and full disclosure are factors in the consideration of the existence of a conflict of interest.

2. MONITORING/MANAGING CONFLICTS OF INTEREST

A licensee should examine whether a conflict of interest exists, not only at the outset of a relationship with a client, insurance company, or other principal, but throughout the duration of the relationship, as new circumstances or information may establish themselves during that period which could reveal or lead to a conflict of interest.

Where there is a conflict of interest, or the potential for one, a licensee has a responsibility to address the conflict with the client, insurance company, or other principal before the transaction is completed, or, if the conflict is not identified until after the transaction, as soon as reasonably possible.

3. DISCLOSURE OF CONFLICTS OR POTENTIAL CONFLICTS OF INTEREST

A licensee has an obligation to provide appropriate disclosure to a client, in sufficient detail, of all real, potential, or apparent conflicts of interest to ensure a client can make an informed decision regarding an insurance transaction. The standard of disclosure should be reasonable and prudent for the circumstances. Disclosure should include an explanation of the conflict of interest, its relevance to the insurance transaction, and be provided to the client prior to the client making a decision whether to proceed with the insurance transaction. In all cases, when disclosure is required, it should be made in writing.

When there is an irreconcilable conflict between a licensee's duty to a client, an insurance company, or other principal and other duties or responsibilities the licensee may have, the licensee should decline to act, even with consent.

Insurance agents are also required to comply with the disclosure requirements contained in the

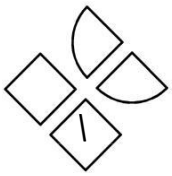
Marketing of Financial Products Regulation under the *Financial Institutions Act*. The disclosure requirements apply every time an insurance transaction takes place. The disclosure requirements must include the following:

a) The name of the insurance company whose service or product is being provided.

b) Any relationship (over and above the contractual relationship to represent) between the insurance company and the licensee offering to provide the service or product (e.g., a financial institution has loaned funds to the licensee to finance his or her insurance or other business).

c) Whether a commission or compensation is to be paid by the financial institution to the licensee offering to provide the service or product.

d) Before acting as an insurance agent, disclosure to the public that the licensee is an insurance agent.



4. NEED FOR A CLIENT'S EXPRESS CONSENT

Where there is a conflict of interest, or the potential for one, a licensee should either not act in the transaction; or where the licensee believes he or she is able to properly represent the client, insurance company, or other principal without the conflict having a material or negative effect on the representation of that party, the licensee must act only where express consent to the conflict from the appropriate parties is obtained.

In such cases, Council recommends that the client, insurance company, or other principal's express consent be obtained, in writing, or, in the alternative, that the licensee confirm to the appropriate parties, in writing, the discussion that occurred regarding express consent.

Express consent must be informed, voluntary, and should take place only after all appropriate disclosures have been made. Disclosure is an essential requirement in obtaining consent. A licensee must inform the relevant parties of the circumstances and the reasonably foreseeable ways in which a conflict of interest could adversely affect the relevant parties interests. Such a disclosure would include the licensee's direct or indirect relationship to all parties and any interest or connection with the relevant matter. Only after the appropriate disclosure has been provided should the relevant parties be required to determine whether or not to give consent.

Where it is not possible to provide a client, insurance company, or other principal with adequate disclosure because of reasons such as confidentiality, a licensee should decline to act in the transaction and the relevant parties should not be afforded the opportunity to determine whether or not a conflict exists.

In all cases where a conflict of interest exists, or may exist, a licensee must reasonably believe that he or she is able to represent a client, insurance company, or other principal without the conflict having a material or negative effect on the licensee's representation of, and duty to, the relevant parties. It is recommended that, in such cases, the licensee clearly document why he or she believes that he or she can reasonably represent the relevant parties. This documentation should be provided to the relevant parties and maintained in the licensee's file.

5. EXAMPLES OF CONFLICTS OF INTEREST

While not intended to be an exhaustive list, the following are some examples of conflicts which may arise.

I. All Licence Classes

Situations may arise where a licensee:

- has a personal, private, financial, or professional interest that will, or could, prevent the licensee from being able to objectively exercise his or her duties and responsibilities to a client, principal, or insurance company. A licensee's personal, private, financial, or professional interest includes, but is not limited to, a direct or indirect financial interest in

the outcome of any transaction or subject matter involving a client or the interests of a family member, employee, business partner, or associate.

- is in a position to take advantage of a client or consumer's inexperience, age, lack of sophistication, lack of education, language barrier, or ill health.

- uses misleading, unnecessary, and/or confusing sales material.

- may derive personal or private benefit by placing insurance business with a particular insurer because some form of financial relationship exists between the licensee and the insurance company, such as ownership or a loan.

- is in a position to give or receive an inducement to or from a third party (a third party being a person other than the client or the insurance company involved in the transaction).

- engages in other employment, job, or business activity ("business activity").

While it is acceptable to engage in a business activity while holding licence, there are business activities that may include real or perceived positions of power or trust. Some examples include immigration consultant, priest or pastor, teacher, doctor, and police officer. As an example, should a teacher be permitted to solicit insurance to the parents of his or her students or a priest or pastor be permitted to solicit members of his or her congregation?

Council, as part of its licence application process, requires applicants to disclose any (non-insurance) business activity. Council reviews such disclosures to determine if the business activity represents the potential for a conflict of interest.

Council has identified a number business activities which it has determined have the potential to be, or are, in a conflict of interest with the duties of those holding an insurance licence. In some cases, the conflict has been determined to be so significant that Council has declined to grant a licence, and, in other cases, Council has been able to address the conflict by placing conditions or restrictions on a licence. To assist licence applicants, Council has posted on its website a list of business activities it has determined are, or may result in, a conflict. This information is updated regularly and can be found with the Code of Conduct at

http://www.insurancecouncilofbc.com/PublicWeb/CodeofConduct.html.

The purpose of this list is twofold: to ensure licence applicants are aware, before commencing the licence application process, that a business activity may prevent them from obtaining a licence; and to provide life agents with details on employment or business activities that Council views as creating, or having the potential to create, a conflict of interest.

For those who commence a business activity at some point after being granted an insurance licence, the responsibility rests with them to identify if the business activity creates, or has

the potential to create, a conflict of interest, and to ensure they govern their insurance practice in accordance with past Council decisions.

II. Life and Accident and Sickness Insurance Agents ("life agent")

i. Membership in an organization where charitable giving is involved

A life agent, who is also an influential member of an organization (e.g., deacon in a church or board member of a charity) and who engages in marketing of insurance as part of a charitable gift giving program for that organization, is in a position to create a conflict of interest. A life agent's position of power or trust within the organization affects his or her ability to provide unbiased advice and a client's ability to make a balanced and informed decision. In such a situation, it would be prudent to use the services of a life agent that is not part of, or associated with, the organization.

ii. Referral arrangements where some form of compensation to or from a third party is involved, including the sale of financial products and the giving of expert advice

Any time a life agent pays a fee to a third party as a result of an insurance transaction, the client must receive written disclosure of this fact before the insurance transaction is completed. The same is also appropriate where a life agent will receive a fee, or other form of compensation, from a third party (over and above the usual compensation received from an insurance company) as a consequence of conducting an insurance transaction. In such circumstances, written disclosure should be provided to the client, and possibly the insurance company, prior to the completion of the insurance transaction.

iii. When representing multiple interested parties

There are many scenarios where this situation can apply, with married couples, families, and business partners being a few examples. While a conflict may not exist at the outset, a divorce or a dissolution of a business partnership can result in a conflict. Acting for all parties in these situations, even if all parties agree, can lead to a conflict. In such cases, a life agent should consider whether he or she should only represent one of the parties and assist the other in obtaining insurance advice from an arm's-length insurance agent.

Conflicts can also arise when a life agent is asked to be the sole executor for an estate, particularly when he or she is also a beneficiary or continues to act as a life agent for the estate. In such cases, a life agent needs to consider whether to continue to act as the life agent or bring in an arm's-length life agent to represent the estate. Similar issues can arise where a life agent has been granted a power of attorney for a client. Should the client no longer be able to manage his or her affairs, continuing to exercise the power of attorney and act as the life agent creates a conflict of interest.

iv. Moving a client from one insurer to another

If the reason for moving a client from one insurance company to another is because a life agent no longer represents the original insurance company, the client needs to be advised of this, even if it is not the primary reason for the change.

v. Involving a client in investing in an insurance agency or other business activity

Any discussions with a client about investing in, or loaning money to, a life agent, a life agent's insurance business, or another business venture is a conflict of interest. Such discussions should only occur when the client is represented by independent legal and financial advisors. If a client refuses to obtain independent legal advice, the investment or loan should not occur.

The same requirements would apply if a life agent were to loan money to, or invest in, a client, a client's business, or a related business venture.

III. General Insurance Agents and Salespersons ("general insurance licensee")

i. Direct or indirect interest in related businesses (e.g., restoration and construction companies, building supply companies, and salvage companies)

Where a general insurance licensee has an interest in a business that may be recommended to a client as a result of a loss, claim, or another insurance transaction, the client and the insurance company on risk should be advised of this interest prior to the transaction occurring.

ii. Any financial interest a general insurance licensee has in an insurer or vice versa.

See Section 3 of this Appendix regarding required disclosure.

iii. Moving a client from one insurer to another

If the reason for moving a client from one insurance company to another is because a general insurance licensee no longer represents the original insurance company, the client needs to be advised of this, even if it is not the primary reason for the change.

iv. Involving a client in investing in an insurance agency or other business activity

Any discussions with a client about investing in, or loaning money to, a general insurance licensee, a general insurance licensee's insurance business, or another business venture, is a conflict of interest. Such discussions should only occur when the client is represented by independent legal and financial advisors. If a client refuses to obtain independent legal advice, the investment or loan should not occur.

The same requirements would apply if a general insurance licensee were to loan money to, or invest in, a client, a client's business, or a related business venture.

IV. Insurance Adjusters

i. Direct or indirect interest in related businesses (e.g., restoration and construction companies, building supply companies, and salvage companies)

Where an insurance adjuster has an interest in a business that may be recommended to a client as a result of a loss or claim, the insured and the insurance company should be advised of this interest at the time of the recommendation.

In addition, if an insurance adjuster has a relationship or understanding with a contractor, restoration company, or service or product supplier that may result in some form of compensation, gift, or inducement being paid because of a referral by the insurance adjuster, the insured and the insurance company should be advised of this interest at the time of the recommendation.

ii. Relationship – a proper explanation to an insured that the insurance adjuster "works" for the insurance company

While an insurance adjuster has duties to an insured during the claim process, the insurance adjuster is usually contracted to represent the insurance company. The insured needs to know and understand that the insurance adjuster's primary duty is to the insurance company. This relationship needs to be explained to the insured at the first meeting.

iii. Relationships that may exist between the insured and the insurance adjuster

Where a relationship exists between an insurance adjuster and an insured, the insurance adjuster must disclose this relationship to the insurance company before commencing to adjust the claim.

CLIENT CONFIDENTIALITY GUIDELINES

FOR INSURANCE AGENTS, ADJUSTERS, AND SALESPERSONS ("Guidelines")

Maintaining the privacy and confidentiality of client information is one of the cornerstones of the insurance industry. The insurance industry is built on trust and clients expect that when they provide their personal information for the purposes of an insurance transaction, the information will be properly protected and will only be used for the purpose for which the information was provided, unless the client expressly authorizes otherwise.

In 2009, Council issued Notice ICN 09-003 *Penalties for Unauthorized Access of the Insurance Corporation of British Columbia's Database* advising licensees there would be no tolerance for intentional unauthorized access to, or use of, a person's information. Since then, Council has identified situations where licensees failed to appreciate that even seemingly innocuous activities could result in a breach of privacy.

The purpose of the Guidelines is to assist licensees in understanding client confidentiality requirements, which involve a number of factors pertaining to the collection, use, disclosure, storage, and destruction of clients' personal information.

Licensees should make themselves aware of these factors and ensure they are accounted for in their day-to-day operations. Ideally, licensees should have written policies and procedures governing client privacy and take reasonable steps to ensure that all staff are aware of these policies and act accordingly.

I. DEFINITION OF PERSONAL INFORMATION

A client's personal information is defined as all information collected by a licensee about the client, excluding publicly available contact information.

II. USING CLIENT INFORMATION

In accordance with Council Rule 7(1), a licensee cannot divulge or use any information derived from a client, except for the purpose for which the information was obtained, unless expressly authorized by the client or as required by law.

III. Express Client Authority

Express authority from a client must be clear and leave no dispute that the client has allowed a licensee to use or disclose his or her personal information for a specific purpose other than the purpose for which the information was given or intended.

•

Council acknowledges that express authority can be given either orally or in writing, but recommends that, whenever possible, it be obtained in writing from the client or, if given verbally, subsequently confirmed with the client in writing by the licensee. Without written express authority, it is difficult for a licensee to demonstrate that he or she acted appropriately should a concern arise regarding the handling of the client's information.

Without express authority from the client, the following situations would be a breach of Council's confidentiality requirements:

- A client's information is used or accessed by a licensee, either directly or indirectly, for purposes other than what it was collected for.
- A licensee uses a client's information to promote the licensee's services or products.
- A licensee provides information upon request about a client to a licensee who works at a different agency.
- A licensee provides information about a client to the client's spouse, relative, or friend, regardless of the reason.
- An insurance adjuster provides information about an insured to the insured's insurance agent.
- A licensee shares a client's information with a third party so that the third party can offer another service to the client.

The above examples are not meant to be exhaustive, but are intended to demonstrate that an action, no matter how innocuous, could be a breach of client confidentiality.

IV. PROTECTING CLIENT INFORMATION

A licensee has a duty to safeguard all of a client's personal information that is in his or her possession. A licensee is responsible for determining the appropriate safeguards necessary to meet this duty. Such safeguards must address the accumulation, storage, and, when appropriate, disposal of a client's personal information.

As an example, disposal of a client's personal information in a manner that could expose the information to access by any unauthorized party, intentionally or otherwise, would constitute a breach. Disposing of personal information in a garbage or through a shredding service, where the service provider does not have appropriate confidentiality protocols in place, would be considered breaches.

•

V. SALE OR TRANSFER OF CLIENT INFORMATION

Section 20 of the *Personal Information Protection Act* ("PIPA") provides direction on what is required if a licensee's book of business is being sold to another licensee. In summary:

A licensee may disclose personal information about clients, without their consent, to a prospective purchaser ("third party") of the clients' information, if it is necessary for the third party to determine whether to purchase the licensee's book of business. However, this may only occur if the licensee and the third party have entered into an agreement that limits the third party's use or disclosure of the clients' personal information solely for purposes related to the purchase of the book of business.

If a licensee proceeds with a sale of a book of business, the licensee may disclose, without consent, clients' personal information contained in the book of business to a third party on the condition that the third party may only use or disclose the personal information for the same purposes for which it was collected, used, or disclosed by the licensee and is limited only to the personal information covered by the business transaction. In addition, the clients whose personal information was disclosed must be notified the business transaction has taken place and personal information about them has been provided to the third party. *In such cases Council recommends that the disclosure to the clients be timely (30 calendar days after completion of the sale) and in writing.*

If the sale does not proceed or is not completed, the licensee must ensure the clients' information is appropriately destroyed by the third party or returned to the licensee.

Orphan Clients – Reassignment of Life Insurance Policies

When an agency (for the purposes of this section an agency means a life insurance agency or a life insurance managing general agent) knows the Agent of Record ("AOR") for a policy is no longer available to service the client, it may assist in the reassignment of the policy to another licensed agent.

An agency may take an active role in this process by informing the client that their AOR is no longer an insurance agent or has ceased to represent the agency and by offering to assist the client in

reassigning their policy to a new AOR. In such situations, the client has the option of declining the agency's service and can elect to find their own AOR.

The appointment of a new AOR by an agency should not occur without first notifying the client and no personal information should be provided to a (potential) new AOR without first obtaining the client's consent. The recommended process of client notification is by way of letter, advising them of the status of their AOR and what is required to obtain a new AOR.

•

VI. AGENCIES, FIRMS, AND NOMINEES

It is the responsibility of insurance agencies and firms and their nominees to ensure their licensees and employees understand the confidentiality requirements and that appropriate measures and safeguards are in place to protect personal information.

Such measures should include:

- Periodic reviews and testing of how clients' personal information is managed and handled.
- Appointing an appropriate person to oversee the agency's or firm's duties in this regard.
- Implementing strict procedures on the management and handling of personal information.

VII. PRIVACY LEGISLATION

Council's position and requirements on client privacy and confidentiality do not override the requirements under existing legislation. Rather, the Guidelines are intended to emphasize to licensees the importance of client privacy. Licensees are reminded that PIPA governs their activities, which includes requiring that:

- A licensee designated one or more individuals to be responsible for the licensee's compliance with PIPA.
- Policies and practices be developed to ensure compliance with PIPA.

Manulife Code of Conduct

Manulife Introduction

At Manulife Financial, we value our good name and constantly strive to apply high standards of integrity and professionalism to everything we do. Operating in an ethical manner is essential to our success. Since much of our success can be attributed to the quality of business sold by our Advisors and to the excellent service provided to customers, we rely on you to preserve out shared reputation for the fair and ethical treatment of clients and the public.

Our vision:

Rooted in Manulife Financials corporate values, our market conduct and compliance is:

To create and promote a culture of compliance and ethics within our distribution channels and with our internal partners where everyone takes personal ownership for achieving and maintaining an environment in which compliance and ethical conduct are an integral part of the decision making process.

Advisors of Manulife Financial hold a position of trust and responsibility when engaging in the promotion, distribution, sale, and servicing of our products. The actions of an Advisor can affect the reputation of other Advisors, Manulife, and our industry. Manulife's Code of Business Conduct provides direction when dealing with applicants, clients, claimants, and the general public. This Code of Market Conduct for Advisors expands upon certain portions of the Company's Conduct as it relates to Advisors.

Purpose

This Code of Market Conduct ("Code") contains general principles and standards that should govern the conduct of Advisors, in their business relationships with applicants, clients, claimants, and the general public as well as regulators, other supervisory bodies, and Manulife.

In this Code:

"The Company" means the Manufacturers Life Insurance Company (Manulife Financial), Canadian Division, and its affiliates.

"Agreement" means any contract or document or amendments thereto, under which any person is authorized to promote, sell, or service the Company's products or services.

"Advisor" means a person who has entered into or is operating under an Agreement with Manulife Financial.

"Client" means current or prospective applicants, claimants, beneficiaries, or any person who is currently engaging the Advisor in their capacity as an Advisor, or where applicable, members of the Public.

Obligations of an Advisor

The authority and obligations of an Advisor are defined by the Agreement. This Code forms part of the Agreement. However, if there is an inconsistency between this Code and the Agreement, the Agreement governs, to the extent of the inconsistency. Compliance with the Agreement means that the Advisor must know, understand and adhere to:

- The Agreement
- This Code
- Industry codes or guidelines that apply to Advisors
- The Company's Code of Business Conduct as it applies to Advisors

- Any rules, policies, or directives communicated by the Company from time to time. Each of the general principles below is followed by a series of related standards. In some cases, specific examples are included to clarify the application of a standards. Omission of a particular standard or example should not imply that it is not important or applicable. Advisors should always consult the additional resources made available by the Company if questions arise.

Relationship with Clients and the Public

Advisors shall act in the best interest of clients, and deal with them honestly, fairly, and professionally.

An Advisor Shall:

Competence and Professionalism

1. Meet and maintain industry standards of proficiency.
2. Meet any certification requirements of the Company.

Priority of Client's interest

3. Always put the interest of the client before their own. Therefore, and advisor must:
    a. Not replace, or induce the lapse, transfer, redemption or surrender of any existing or pending business without conducting a complete analysis, disclosing all costs and proposed benefits to ensure that the proposed transaction is in the Client's best interest. Any replacement, redemption or transfer of business shall conform to all regulatory and Company Requirements and Guidelines.
    b. Not allow themselves to be placed in a conflict of interest position. All conflicts of interest or apparent conflicts of interest must be disclosed to the client. The Advisor should decline to act if a reasonable person would conclude that the conflict of interest could compromise their objectivity. For Example: An Advisor must not
        i. Accept an appointment as Trustee, Executor, or Attorney under Power of Attorney for a client, other than in accordance with the policies of the Company;
        ii. Enter into a debtor/ creditor relationship with the client;
        iii. Assume ownership of a client's policies or accounts.

Make appropriate recommendations

4. Exercise due care and thoroughness in making recommendations and when discussing material changes with clients.
5. Ensure that they have made a diligent and business-like effort to collect and analyze information relating to the client's needs, objectives and financial circumstances. The information should be updated as necessary.
6. Not make recommendations unless it has been determined that it is appropriate in light of the client's needs, objectives, financial situation, and experience, and is in the client's overall best interest.

7. Not make a recommendation or transact any business unless they have the appropriate proficiency, registration or licensing to do so.
8. Make a reasonable and diligent effort to ensure that the client understands the nature and purpose of the recommended transaction, including the associates benefits, risks, costs, charges, and restrictions.
9. Not exercise discretionary authority over a client account, nor solicit or accept any document, instruction, or direction in which the client gives the Advisor such authority, except those limited authorizations which are explicitly permitted by the Company's policies and procedures.
10. Maintain sufficient information in client files to demonstrate the appropriateness of any sale or any advice given and retain all material information which was utilized in all negotiations, continuance or maintenance of a policy or contract.
11. Make reasonable and diligent efforts to avoid any misrepresentation in any recommendation. Advisors who use their own illustrations or presentations in addition to those provided by the Company should have them reviewed by the Compliance before presenting them to a client.

Proper Disclosure and Delivery

12. Not make any misrepresentation or false or misleading statements.
13. Ensure fair and adequate disclosure of all facts reasonably available and necessary to enable clients to make an informed purchase or decision. This includes but it is not limited to:
    a. Information about the Advisor (e.g. holding out requirements, licensing or registration);
    b. Information about the Advisor's relationship with the Company (e.g. title, compensation);
    c. Information about the products and services offered as an Advisor of the Company (e.g. type, benefits, risks, costs, assumptions, illustrations, tax implications, conditions, etc.);
    d. Disclosure of hen the Advisor is or is not acting on behalf of the Company;
    e. Disclosure of information required by the Company, by law or by regulation.
14. Ensure that the client obtains all required point of sale documents supplementary information, including summary information folders, illustrations, disclosure documents, client copies of application forms or other collateral materials.

Client Service

15. Provide service promptly, accurately, and thoroughly.
16. Properly supervise any employee who is providing services to clients.
17. Provide conscientious service after a sale, including:
    a. The Prompt
        i. Delivery of all policies and account documentation to the client.
        ii. Return of all required documentation to the Company.

iii. Completion of any requests to provide additional information required by the Company.

b. Periodic review of client accounts, to ensure that their needs continue to be met.

Collection and Protection of Clients Personal Information

18. Comply with privacy legislation, and adhere to the Company's Privacy & Confidentiality Code and Privacy Policies.
19. Obtain only such information or documentation that is required to:
    a. Determine the identity of clients
    b. Make appropriate recommendations
    c. Complete applications or other forms
    d. Provide client service
20. Collect, use, and disclose information only for the purpose for which it was obtained and only with a client's consent, except where disclosure is authorized by law, or the Agreement.
21. Ensure that confidential information is properly disposed of, where no longer required.
22. Make a reasonable effort to design and manage procedures and systems to protect confidential information from error, loss and unauthorized access or disclosure.
23. Promptly return any documents or other property, including policy and account documents, belonging to the client.

Relationships with regulators

Advisors must know, understand and abide by the letter and spirit of Federal and Provincial Laws and Regulations that govern their activities. This means an Advisor shall:

1. Understand and comply with all applicable laws, rules, and regulations of any government, governmental agency, regulatory organization, licensing agency, or industry or professional association governing their professional activities or the industry in general.
2. Not knowingly condone, participate in, or assist any violation of any laws, rules, regulations, or Company policies.
3. Not engage in any conduct involving dishonesty, fraud, deceit, misrepresentation, unfair or deceptive acts or practices, or commit any act prohibited by law, or the Company.
4. Co-operate fully with regulators in any investigation or disciplinary hearings.

Relationships with the Company

The Company must be able to rely on the accuracy and authenticity of information and documentation provided by the Advisors. Advisors must understand and abide by the obligations and limits of their authority to act on behalf of the Company. For example, Advisors are not authorized to accept risks, amend policies or accounts, waive policy or account provisions, incur debts, or contractually bind the Company in any manner.

An Advisor shall:

Representation of and to the Company

1. Act with utmost goof faith, in all dealings with the Company.
2. Immediately notify the Company in writing
    a. Of any interaction with regulators that is outside of the ordinary course of business.
    b. Of any material changes in their circumstances that may impact their sustainability as an Advisor (e.g. criminal charges or convictions, bankruptcies, license lapsing, etc.)
    c. Of any actual or threatened client complaints, claims, or other enforcement action or legal proceedings.
3. Co-operate with and be responsive to requests from the Company, including but not limited to, investigations relating to their business practices or conduct.

Practice Management

4. Make adequate arrangements to ensure that staff are suitable, adequately trained and supervised, and that well-defined compliance procedures are in place.
5. Organize and control their business practice in responsible manner by keeping proper records, and in such a manner to enable the Company to have access to these records at all time.

Privileged Information

6. Not represent the Company to the media unless expressed authorization is obtained from the Director of Media Relations.
7. Not disclose or misuse proprietary, sensitive or confidential information about the Company, its products, services or procedures. This includes copyrighted materials, software, online information, etc.
8. Guard against the inappropriate use of any information (e.g. insider trading).

Duties with Respect to the Sale of Products

9. Make appropriate product recommendations to the client.
10. Provide proper disclosure and documentation to the client.
11. Remit to the Company promptly all premiums, or funds collected from clients on behalf of the Company, for the purchase or servicing of products offered for sale by the Company. Advisors must ensure that all cheques and money orders are made payable to the Company.
12. Fully disclose to the Company any new information regarding an application or a claim, which is obtained after the sale and prior to delivery and acceptance by the client (e.g. a change in the medical history of the applicant).
13. Take appropriate steps to conserve existing business, except where it is not in the client's best interest.

Authenticity of Documents and Instructions

Not sign, or knowingly permit someone else to sign for, represent or authorize any transaction in the name of any other person, even with the consent of that person, except where such authorizations are exercised using a valid Power of Attorney or other permitted client authorization.

Not sign as a witness, or knowingly permit another person to sign as a witness, unless the Advisor or other person is physically present when the document is signed and has confirmed the identity of the person signing the document.

Not ask a client to sign blank forms. Advisors must always ensure that all material parts of forms and applications are fully completed before they are presented to the client to be signed.

Not process or submit to the Company under the Advisor's name, business which was actually sold or transacted by a person other than that Advisor, whether or not the other person is licensed or is an Advisor of the Company. This activity is referred to as fronting.

Not record false or misleading information on any form or application, or allow a form to be submitted that they know or ought to know contains false or misleading information. For example, where the Company's rules permit Advisors to verify client instructions by means other than a personal visit, the Advisor must record the actual date and time of the contact.

Not submit a transaction unless they have made a reasonable and diligent effort to ensure that the client understands the nature and purpose of the recommended transaction, including the associated benefits, risks, costs, charger and restrictions and the client has explicitly authorized the transaction. Supplementary documentation should be retained in the client file.

Effect of Non-Compliance with this Code

In order to protect its reputation that of its Advisors, and the best interest of the public, the company will take appropriate action against any Advisor(s) who have been found to have violated this Code. This may include filing a report of unsuitability with the industry or regulatory bodies, contract termination with or without cause, filing a complaint with the police, or a litigation against the offending Advisor(s) where the Company has incurred losses caused or contributed to by the Advisor.

Remarks by Jeanne M. Flemming, Director,

Financial Transactions and Reports Analysis Centre of Canada, to the Canadian Life and Health Insurance Association

***Proceeds of Crime (Money Laundering) and Terrorist Financing Act*: Why Compliance with the Law Matters**

Toronto

May 13, 2010

Check against delivery

Introduction and Outline

Thank you for that introduction

I would like to thank Frank Swedlove for inviting me to speak today. Frank has been a long-time leader in Canada's efforts to combat money laundering and terrorist financing. As president of the Financial Action Task Force, he worked globally, upholding the standards to which each country strives in their anti-money laundering and anti-terrorist financing regimes. I think you are fortunate to have him as the president of your association.

FINTRAC is part of a larger global effort. Every country in the world, perhaps with a few notable exceptions, is engaged in finding ways to protect the legitimate financial system from those who would abuse it—finding ways to detect and deter and prevent money laundering and terrorist activity financing.

At the root of Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* are those concepts of detection and deterrence and prevention. That's why the law created reporting compliance obligations for reporting entities like yourselves and FINTRAC to ensure compliance with those obligations.

At FINTRAC, we find ourselves squarely between the businesses that provide financial transaction reports to us and the police and other investigators who benefit from the financial intelligence we produce. Being in the middle, we add value to the information that is provided; we move it further along and offer real insight to assist the investigation of serious crimes.

I want to provide you an update this morning that will give you some context to explain how this effort is working. I realize there have been a few questions about this initiative and perhaps a few myths floating around. That may be the consequence of being a financial intelligence agency that operates behind the scenes. At FINTRAC, we do guard our information very closely.

One myth I would like to dispel this morning involves criminal convictions. FINTRAC does not lay charges. FINTRAC does not prosecute. Trying to measure FINTRAC by convictions would be similar to asking a roomful of lawyers and compliance officers what their sales numbers were last year.

FINTRAC is in the business of assisting investigations, not conducting them. We do that by getting relevant financial intelligence into the hands of those that investigate crime. We assist investigations every day, making use of the information that is reported to us. Taking all the financial transaction information that we have at our disposal and bringing analysis to bear in turn—analysis which identifies criminal proceeds and providing some useful financial intelligence to the investigations and prosecution.

I realize that many of you have a long tenure in this business. I would like to emphasize that when it comes to money laundering, it is simply the proceeds of crime re-entering the legitimate financial system. It is any attempt to transport, conceal or otherwise convert those proceeds of crime. I would encourage you to approach the problem of money laundering as one that related to all those crimes that can generate criminal proceeds, such as drug trafficking and fraud.

FINTRAC does spend a considerable amount of time and resources working on money laundering cases where fraud is the original predicate offence. And we make use of all the information that is reported to enable us to conduct our analysis and ultimately make our disclosure to assist the criminal investigation. We are only as good as the information we have and our ability to analyze it.

When it comes to deterrence and prevention, the work that FINTRAC does to ensure compliance with the law strives to keep illicit funds from entering the legitimate Canadian financial system. This involves ensuring that proper records are kept, that identification is obtained, that risks are being assessed and the other elements of a compliance regime are in place.

All the entities that make up Canada's financial system have a stake in ensuring that the level of deterrence is high. Life insurance companies have a stake in this too.

When it comes to detection, FINTRAC's intelligence assists investigations and it assists prosecutions. Financial intelligence sheds light on the transactions that can be related to criminal activity. It assists investigators in making decisions about where to seek evidence, who to include or exclude as part of the investigation, how the targets are connected and where the assets may be hidden.

I'd like to give you a reference point for how we search transactions that we suspect to be relevant to money laundering in our database of more than 100 million transaction reports. Let me say that searching this information is like looking for a needle in a haystack, in a field

of haystacks. On their own, transactions linked to criminal activity may not stand out or be noticeably different from millions of innocent transactions. However, we have developed data mining tools and methodologies over the years that enable us to detect patterns of suspected money laundering and to start following the money trail.

The other thing that can guide us is information we receive from law enforcement and other agencies—as part of ongoing investigations that may have already identified targets. In these cases, we can start from what is known and shed light on the existing investigation. Roughly 80% of the time, information from investigative agencies is the starting point for our disclosure of financial intelligence. This ratio may change over time. For the moment, the demand to assist ongoing investigations is high. High demand from prospective recipients does speak well of the product.

The financial intelligence that we produce can be complex and it can show the great efforts that criminals go through to hide the source of their funds. We have cases where the suspected criminals have used up to 16 or more financial institutions across the country to disperse and hide their assets. Being the recipient of financial transaction reports from across the country, and having access to information from other financial intelligence units from other countries, does give us an advantage when trying to piece together the money trail.

The Problem That We Face

Before becoming FINTRAC's director, I was not aware of the extent of the lucrative criminal enterprises that appear to be operating in this country. Seeing cases each day has had some affect on me. After two years in this job, I am occasionally asked what things preoccupy me, or more specifically, what are the questions that keep me up at night. For me it comes down to "are we doing enough to make this country a hostile place for those that launder money and finance terrorist activity?"

There are criminals in this country and they are getting up to some pretty bad things. They are fleecing and defrauding some of the most vulnerable members of our society, committing fraud, they are selling drugs, corrupting institutions. And, when it comes to mortgage fraud, they are stealing whole houses. We are not talking about petty crime here; some of these criminal activities appear to be large ongoing enterprises with a damaging impact on our society. The victims also include the institutions you represent.

I feel I have to make this point about the scale of criminal activity in this country because it concerns me. Perhaps that is a function of working at FINTRAC and of having a perspective on the many criminal investigations and the money that seems to be moving in these suspected criminal networks. It can be disheartening, at times.

This perspective has brought me to the view that Canadians can be naïve and perhaps overly optimistic in their view that crime and, in particular, organized crime are not Canadian

problems. I want to assure you that they are and that they have an impact on Canada's communities large and small. Crime affects us all. Even those of us who are not victims of fraud or theft will feel the residual effects in a system that is compromised by the presence of a criminal element.

I want to call your attention to the larger Canadian financial system and the role that you have as operators within it—and as the stewards and occasionally gatekeepers of this system.

Those of you who work with insurance products must surely have your own perspectives on crime and perhaps a perspective on fraud and money laundering within your own industry. I want to make the connection between money laundering and fraud very plain because too often money laundering is viewed as an esoteric subject removed from the real crimes that produce real profits.

Financial intermediaries, such as brokers or agents, can actually do something to make it more difficult to operate a criminal enterprise in this country. You have that opportunity. It is an opportunity to strengthen the integrity of Canada's financial system and to shut out the criminals that would abuse and exploit this system. At the same time, it may also help curb frauds committed against insurance companies in this country.

The connection that I want to make for you is that any fraud against an insurance company will generate criminal proceeds that must be laundered. Even if those proceeds are in the form of a cheque from an insurance company, it is still criminal proceeds. When that cheque is carried to a bank or credit union, depositing that cheque is money laundering. Transferring those criminal assets to another account, that is money laundering too.

So, why does it matter that businesses send us reports?

It is important because the police don't have our unique data base to follow the money trail. FINTRAC provides the leads and the information necessary to assist police in acquiring search warrants. FINTRAC's information can also reveal new targets for an investigation and previously unknown connections between individuals, bank accounts and companies. We also have an international perspective on transactions that is made possible by the reporting of electronic funds transfers and from the exchanges of information with financial intelligence units in other countries—both of which assist in following money into other jurisdictions and from those jurisdictions to Canada.

When your business sends in a suspicious transaction report it is important to keep in mind that several other institutions, in a variety of financial sectors, may have also provided reports about the same individual. As I mentioned earlier, we have cases in which 16 different financial entities have been used to obscure the trail of the money from its criminal origin to its final destination. Last year, 43% of our case disclosures involved reports from six or more reporting entities. So, as you can see, the cases can be complex and the transactions are

seldom limited to a single institution. This highlights the benefit of collecting the data in one place and analyzing it with other contextual information like corporate registry information and other open-source data. It is particularly satisfying when we have the information at our disposal that allows us to connect these dots and then be able to show the money trail to police.

We also do the same for our international partners who are interested in transactions that occur in Canada that can have some significance to criminal investigations in other countries. Money moves easily around the world, FINTRAC plays a role in cooperating with financial intelligence units in other parts of the world, helping the global effort to curb the flow of illicit money and to detect criminals through their financial activity. As of today, we have entered into agreements to share information with the financial intelligence units of 69 other countries. This has opened a window on financial activity beyond our borders that also benefits Canadian investigations.

FINTRAC disclosed 556 cases to investigators last year, more than any previous year. These case disclosures, which involved more than 100 thousand transactions, were supplied to assist investigations of money laundering related to drug trafficking, fraud, smuggling of contraband, terrorist activity financing and a variety of criminal activities that can generate the proceeds of crime. We provided this intelligence to federal, provincial and municipal police forces. We also provided intelligence to CSIS, the Canada Border Services Agency, Canada Revenue Agency and to our international partners during the year.

Looking at all these cases as they are pulled together by FINTRAC's analysts, it is truly remarkable the lengths to which people will go to keep transactions out of their own name or to have nominees carry them out on their behalf only to have the funds ultimately returned through series of transactions and bank drafts to businesses under their control or accounts held in their name, here or in other countries.

Often the money laundering technique is simply moving the funds into an account and withdrawing them quickly in the form of a bank draft or transmitting the whole amount to a foreign account shortly after the deposit. It can often make no business sense to run the transactions through a series of accounts en route to their end destination but this is also sometimes done.

We have received a suspicious transaction report submitted to us from the life insurance sector that highlights that information can come to your attention long after the initial transaction. When that information does come to light, you may look back at those earlier transactions in a different way. As an example of just such a case, a Canadian life insurance company had written a policy on a man who was subsequently determined to be a notorious criminal. This came to their attention after a very public attempt on the man's life had failed. The newspaper reports detailed his role in the local crime scene, including a history of charges and accusations that had been brought against him over the years.

The insurance company began to wonder why they held the policy, how it got written and if the premiums might have been paid with the proceeds of crime. To be fair, the payments may have seemed normal at the time. Payments were made by cheque. The decision to look back to the original transactions on this policy and report them as suspicious was a good one. The important thing is that once you arrive at a suspicion that proceeds of crime may have entered into the transaction, this should trigger the filing of a suspicious transaction report.

Proceeds of crime can enter the system in a variety of ways. When it comes to insurance transactions, it may simply be a cheque drawn on a bank account. It may be hard to spot. If you have other contextual information, you should add that to your examination of risk.

The Criminal Intelligence Service of Canada estimates that there are 750 organized crime groups in Canada, each engaging in a variety of criminal activities that generate large amounts of money. When it comes to dealing with these groups, we should strive to make their operations more difficult to run and easier to find.

As financial intermediaries in the larger Canadian financial system, your financial agencies and advisors are at the forefront of detecting and deterring the financial transactions that can facilitate the activities of these criminal networks. The transaction reports that you send are critical to this effort, and you are uniquely placed to make this contribution. That is why we have this law.

Diligence is needed to continually foster a culture within your financial agencies and advisors that meets the compliance objectives of the law. This includes effective training. Training is an ongoing activity in every business, and so it should be with your compliance programs.

You should also review your own compliance programs to assess any inherent risks of money laundering and terrorist financing within your business lines and your different products. Once you assess the risks, there is a need to implement controls to mitigate your exposure to such risks. This was the intention of the risk-based approach that was adopted two years ago. It is now a requirement of the law, but the diligence that is required to make it work is an important element as well. As we know, these are not things that can be done once and set aside. They have to be part of the business and an ongoing effort.

There is also a need to identify and to report suspicious transactions. The obligation has been the law for nearly ten years and should not require a reminder. But after ten years, the level of reporting from the life insurance sector remains unusually low. I say that because there has been one exception. There is one company that is reporting more than the rest and the suspicious transaction reports appear to be appropriate. I would like to encourage a race to the top among the life insurance companies assembled here to be diligent in your review of risks within your own product lines and to ensure that you are meeting your reporting obligations.

Looking Forward

And to speak for a moment about the enforcement of the law, in late 2008 FINTRAC gained the power to issue administrative monetary penalties. Also known as AMPs, these fines have been used in the last year where we have identified violations of the law. They are a proportional penalty, one that takes into account not only the nature of the violation but the size of the entity or business that is being fined, their ability to pay and their compliance history.

Administrative monetary penalties serve as an adjunct to existing criminal penalties. This means both criminal and civil penalties will not be issued for the same instances of non-compliance. They are intended to encourage compliance not punish past non-compliance with the law.

These new penalties mark a change in FINTRAC's approach and perhaps in FINTRAC's tone. After ten years of outreach and efforts to raise awareness, there is a greater expectation that businesses should have effective compliance regimes in place and that the requirements of the law should be part of the normal course of business. FINTRAC will now issue penalties when the violation of the law merits such a response.

Looking further out into the future, Finance Minister Flaherty has indicated "the government will be relentless in its efforts to combat money laundering and terrorist financing and that it will do what must be done to protect the interests of Canadians and ensure a safe and strong market for investors here and around the world."

An expression of that commitment came in the 2010 federal budget. FINTRAC's operating budget was increased by eight million dollars to improve our compliance regime and to expand the definition of predicate offense for money laundering to include tax evasion thereby increasing FINTRAC's ability to make disclosures in this area.

With the proposed new funding, FINTRAC will be able to hire new staff and increase the number of compliance examinations that we can conduct. This increase will allow us greater ability to ensure compliance with the law in all sectors. For example, FINTRAC will be conducting enhanced compliance activities involving federally-regulated financial institutions (FRFIs) which will be independent of the OSFI reviews. Our intent is to increase the examination coverage of this sector with a focus on improving the data quality of the reports.

Finally, the 2010 Federal Budget also announced new measures to strengthen Canada's antimoney laundering and anti-terrorist financing regime. These are included in Bill C-9, the *Jobs and Economic Growth Act*, which proposes new authorities for the Minister of Finance to issue directives to advise the financial sector of foreign jurisdictions and entities that pose an illicit financing risk and to require appropriate countermeasures. Under the proposed new authorities, the Government could also limit or prohibit financial transactions with designated

foreign jurisdictions or foreign entities which are found to be at high risk of facilitating money laundering and terrorist financing. This will help ensure that Canada does not unwittingly become the destination of choice for illicit funds looking for a home. For the moment, the legislation has been published and is now available through the Parliamentary Web site.

Thank you for taking the time to listen and thanks once again for inviting me to your conference.