Canada Financial®

*Our Strength is Our People*

# Compliance Manual

Last Revision: July 26, 2018

www.canadafinancial.ca

# 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; and (iii) consistency with best corporate governance practices.

# Recruiting and Selection

**EXPERIENCED**

1. 1st Interview: introduce and showcase the competitive advantage of CF.
2. 2nd Interview: expectations/screening/P100
3. 3rd Interview: decision (subject to the following)
4. Green Grass report ordered
5. Screening: If the following issues apply to a candidate, he/she will not be considered.
    - Compliance record
    - Debit with carrier
    - Production less than $20,000 FYC/yr
    - Integrity/commitment/discipline
    - Two transfers in the past three years
    - Credit and Criminal Record (ICBC)
6. Exceptions to point 5
    - Investigation of compliance record by Chief Compliance Officer
    - No exception for debit
    - Less than required production or excessive transfers
    - Provide a formal business plan
    - Discuss with RVP or CEO

**NEW TO THE INDUSTRY**

1. 1st Interview/Seminar: introduce the career opportunities with CF
2. Invitation to CF seminar
3. 2nd Interview: expectations/screening/evaluation/P100
4. Launch 500/Decision of Hiring
5. Pass LLQP and start CF mentoring program

# 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 carriers' 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
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 crucial 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 advised 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.

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 procedure 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 immediately record the complaint in the complaint log (Please see attached form). 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 Financial's 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 enclosed.*

# 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 contracts with and represent in the field.

Please review the Insurance Council of British Columbia "Code of Conduct "requirements

# 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:
    - license(s) held
    - signature of agent
    - 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 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 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.

The following forms are necessary at point of sale situation:

- Know your client profile
- Reason why letter
- Sales charge disclosure
- Leverage risk disclosure
- Engagement letter

# 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 types 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.

**Requirements 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, CHS, 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
- 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 license period.

# 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 goodwill.

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 if 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 on 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 deciding on 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 our 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; and (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 for 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, the 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 a 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; o loss of

    assets; o financial exposure; or o 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; or o 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 licence 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:

  o any applicable legislation that may require notification; o whether the

  personal information is subject to privacy legislation; o 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;

  - the number of people affected by the breach; whether the

    individuals affected have been notified; and

  - 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 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 Office of the Privacy Commissioner (OPE) 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.

1. Reporting
   1.1. Suspicious Transactions
   1.2. Terrorist Property
   1.3. Large Cash Transactions
2. Record Keeping
3. Ascertaining Identity
4. Politically Exposed Foreign Person
5. Third Party Determination
6. Compliance Regime

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 addresses 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 receive 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 activities?

When determining whether a purpose is to encourage participation in commercial activities, 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 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 (the 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.

**<u>Exemptions to the National DNCL Rules</u>**

**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:
    1.1. Canadian registered charities
    1.2. political parties, riding associations, and candidates
    1.3. newspapers of general circulation for the purpose of soliciting subscriptions 2. calls made to:
    2.1. consumers with whom you have an existing business relationship
    2.2. Consumers who have provided express consent for receiving telemarketing calls 2.3. 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

# Appendices

**Appendix 1**: Insurance Council of British Columbia Code of Conduct

**Appendix 2**: Manulife Code of Conduct

**Appendix 3**: Remarks by Jeanne M. Flemming, Director, Financial Transactions and Reports Analysis Center of Canada, to the Canadian Life and Health Insurance, Association

**Appendix 4**: Annual Self-Review Checklist

The Approach: Serving the client through needs-Based sales practices

IVIC Suitability Needs-Based Sales Practices

Engagement Letter

Investor Profile Questionnaire

Reason Why Letter Sample

Leverage Risks Disclosure Statement

Sales charge Disclosure

Complaints Log