

# New PCMLTFA Obligations

## Securities Dealers

2008

# Presentation Overview

- Introduction
- Objectives of New Requirements
- Changes to Reporting
- Changes to Client Identification and Record Keeping
- New Due Diligence Measures
- Changes to Compliance Regime
- Administrative Monetary Penalty Regime
- Other Information

## Introduction

- The PCMLTFA was amended in December 2006, authorizing the creation of new requirements through its related regulations:
  - *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*
  - *Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations*
- Most new requirements become effective on June 23, 2008

# Objectives of New Requirements

# Objectives of New PCMLTFA Requirements

- Strengthen existing AML/ATF regime and build on FINTRAC's experience
- Address existing gaps in the legislation and regulations
- Enhanced detection and deterrence of money laundering and terrorist financing
- Make illicit transactions more difficult to conduct
- Greater impact against organized crime and terrorists

# Definition

- Definition of “securities dealer”
  - An individual or entity authorized under provincial legislation to engage in the business of dealing in securities **or any other financial instruments** or to provide portfolio management or investment **advising** services
  - “Other financial instruments” include financial instruments such as derivatives

# Changes to Reporting

# Suspicious Attempted Transactions

- Reporting entities will have to report suspicious **attempted** transactions to FINTRAC.
- An attempted transaction is an incomplete transaction that a client intended to conduct and took some form of action.
- An attempted transaction includes negotiations or discussions to conduct the transaction and involves concrete measures taken by either the reporting entity or the client.

## Suspicious Attempted Transactions (cont'd)

- In determining whether an event or activity constitutes a suspicious attempted transaction, consider this:
  - Activity leading to a suspicious attempted transaction is inherently suspicious for money laundering or terrorist financing (mandatory)
  - Presence of key elements of an attempt i.e. intent to conduct a transaction with some form of concrete action
- Every situation is different and should be assessed on a case-by-case basis in light of the facts.

## Suspicious Attempted Transactions (cont'd)

- Example of an attempted transaction:
  - Client attempts to pay for transaction with cash but advisor refuses to accept cash.
- New information to be provided in STR form:
  - whether the transaction was completed
  - if not, the reason why it was not completed

# Changes to Client Identification and Record Keeping

# Client Identification

- If client is present, refer to a valid government-issued identification document

## New Rule:

- Options for ascertaining client identity are expanded in non-face-to-face situations (e.g. telephone, Internet services)

# Client Identification

## New Rule:

- Prohibition to open account if unable to establish identity

# Client Identification: Non-Face-to-Face Methods

1. Use of an affiliate

OR

2. Specific combinations of identification methods.

- cleared cheque
- identification product method
- credit file method
- attestation method
- confirmation of a deposit account

## Affiliate Method

- Method can be used by affiliates.
- An affiliate is a bank, credit union, caisse populaire, trust company, loan company, securities dealer, life insurance company that is either:
  - wholly-owned by the reporting entity;
  - the affiliate wholly-owns the reporting entity;
  - the reporting entity and the affiliate are both wholly-owned by the same entity.

## Affiliate Method (cont'd)

To ascertain identity using this method, must:

1. Obtain the individual's name, address and date of birth.
2. Confirm with affiliate that it has identified the individual with the standard method (government ID).
3. Verify that the name, address and date of birth in the record kept by that affiliate **corresponds** to the information provided by the individual.

## New Non-Face-to-Face Methods

- **Identification product** : Referring to an **independent** and **reliable** identification product that is based on personal information in respect of the individual and a Canadian credit history of the individual of at least six months duration. This type of product can use a series of specific questions, based on an individual's credit file, to enable verification of client identity.
- **Credit file**: Confirming the name, address and date of birth of client by referring to a **credit file** in respect of that individual in Canada that has been in existence for at least six months.
- Products for either of these methods are available commercially, such as those used for credit ratings.

## New Non-Face-to-Face Methods (cont'd)

- **Attestation method:** Obtaining an attestation from commissioner of oaths or guarantor in Canada that they have seen valid identification.
- **Cleared cheque:** Confirming that a cheque drawn by client on a deposit account with a financial entity has been cleared.
- **Confirmation of deposit account:** Confirming that client has a deposit account with financial entity.

# Client Identification: Non Face-to-Face Methods

In non-face-to-face situations, will be possible to:

- Use an affiliate  
**OR**
- One of the following combinations of ID methods:

ID product <b>or</b> credit file	<b>AND</b>	cleared cheque <b>or</b> confirmation of deposit account
attestation	<b>AND</b>	cleared cheque <b>or</b> confirmation of deposit account
attestation	<b>AND</b>	ID product <b>or</b> credit file

## Client Identification: Use of Agents

- Reporting entities may rely on an agent to take identification measures when they have signed a written agreement for that purpose.
- Reporting entities also have the obligation to obtain the customer information from the agent.

# Client Identification: Doubts about Identification

- If a new obligation to ascertain the identity of a client arises for an individual previously identified, a reporting entity is not required to ascertain their identity again if they recognize the individual.
- **However**, reporting entities must ascertain the individual's identity again if they have **doubts** about the veracity or accuracy of the identification information obtained previously.

# Suspicious Transaction Reports

- Reporting entities must keep copies of suspicious transaction reports (STRs) concerning both attempted and completed transactions.
- Reporting entities must take reasonable measures to ascertain identity of the individual who is the subject of a suspicious completed transaction.
  - Except if the individual's identity was previously ascertained or there is a possibility of tipping-off the individual.

## Record Keeping: New Exemption

- If the reporting entity keeps information in a record that is already readily available in any other record kept under the PCMLTFA regulations, they do not have to keep that information again.
- Effective since June 30, 2007

# Intended Use of Account

- For every account opened, must have a record of its intended use.
- Examples of intended use for accounts include the following:
  - long or short term personal savings
  - income generation
  - investment of retained earnings of a corporation
  - market speculation (day trading)

# Record Keeping and Client Identification Exemptions

- New exemptions have been added, for example:
  - The opening of an account established pursuant to the escrow requirements of a Canadian securities regulator or Canadian stock exchange or any provincial legislation.
  - The opening of an account that is opened solely in the course of providing customer accounting services.

# Timelines for Client Identification

- Ascertain identity of individuals authorized to give instructions on an account before any transaction other than initial deposit.
- Confirm existence of corporation and ascertain name and address of its directors within 30 days of account opening.

# Foreign Branches and Subsidiaries

## Foreign Branches and Subsidiaries

- Entities that have branches and subsidiaries located in a non-FATF country must:
  - Ensure that their branches and subsidiaries develop and apply policies and procedures that are consistent with the PCMLTFA record keeping, client identification and compliance regime requirements.
  - If policies and procedures would contravene laws of foreign country for foreign subsidiaries, a record of that fact should be kept.

# Beneficial Owners

# Beneficial Owners

- When required to confirm the existence of a corporation or other entity:
  - Take reasonable measures to obtain information on beneficial owners: all individuals who own or control 25% or more of the corporation or entity.
  - Once obtained, must keep a record of it
  - If not obtained, must record this fact as well.

# Beneficial Owners: Record Keeping

For a corporation:

- Name and occupation of all directors
- Name, address and occupation of all individuals who own or control, directly or indirectly, 25% or more of the shares

For an entity other than a corporation:

- Name, address, occupation of all individuals who own or control, directly or indirectly, 25% or more of the entity

For a not-for-profit organization (in addition to the information above):

- Whether entity is a charity registered with the Canada Revenue Agency (CRA) under the *Income Tax Act* (ITA)

**or**

- an organization other than an ITA-registered charity that solicits charitable financial donations from the public

# Politically Exposed Foreign Persons (PEFP)

# Politically Exposed Foreign Persons

- A PEFP is an individual who holds or has held one of the following offices or positions in or on behalf of a foreign state:
  - (a) head of state or head of government;
  - (b) member of the executive council of government or member of a legislature;
  - (c) deputy minister or equivalent rank;
  - (d) ambassador or attaché or counsellor of an ambassador;
  - (e) military officer with a rank of general or above;
  - (f) president of a state-owned company or a state-owned bank;
  - (g) head of a government agency;
  - (h) judge; or
  - (i) leader or president of a political party represented in a legislature.
- Includes prescribed family members of such an individual.

## Politically Exposed Foreign Persons (cont'd)

- Prescribed family members include:
  - The PEFP's spouse or common-law partner
  - The PEFP's child
  - The PEFP's mother or father
  - The mother or father of the PEFP's spouse or common-law partner (mother-in-law or father-in-law)
  - A child of the PEFP's mother or father (brother, sister, half-brother, half-sister)

## Politically Exposed Foreign Persons (cont'd)

- Must take reasonable measures to determine if a client is a PEFP:
  - At account opening
  - Based on risk assessment for existing accounts that are deemed high risk
- For new accounts, determination must be made within 14 days of account activation.

## Politically Exposed Foreign Persons : How to make the determination?

- Taking reasonable measures means:
  - asking the client; or
  - consulting a credible source of commercially or publicly available information about politically exposed persons.

## Politically Exposed Foreign Persons (cont'd)

- Once PEFP determination is made, other measures apply:
  - Take reasonable measures to obtain source of funds.
  - Obtain senior management approval to maintain account within 14 days of account activation.
  - Must conduct ongoing monitoring of account to identify suspicious transactions.
- A **total** of 14 days to make determination **and** obtain approval.

# Politically Exposed Foreign Persons: Senior Management

“Senior management” means an individual who has the following:

- Authority to make and be held accountable for management decisions about this type of account
- Awareness of the money laundering or terrorist financing risks to which the securities dealer or this type of account is exposed
- Awareness of politically exposed foreign persons

## Politically Exposed Foreign Persons (cont'd)

- 5 elements to keep on record when PEFP determination is made:
  1. Office or position
  2. Source of funds
  3. Date of PEFP determination
  4. Name of member of senior management who approved the account to be kept open
  5. Date of review or approval

# Changes to Compliance Regime

# The Compliance Regime and New Changes

1. The appointment of a compliance officer responsible for implementing the compliance program
2. The development and application of compliance policies and procedures, these will have to be:
  - in writing,
  - kept up-to-date, and
  - for an entity, approved by a senior officer
3. Assess and document the money laundering and terrorist financing risks

## The Compliance Regime and New Changes (cont'd)

4. If the reporting entity has employees or agents, must have an ongoing training program that is in writing and maintained.
5. A review of policies and procedures, training program and risk assessment.
  - Must be carried out every 2 years by an internal or external auditor, or by the reporting entity itself.
  - For an entity, report in writing findings of the review to senior officer including updates and implementation status.

## Risk-Based Approach

- A risk-based approach allows the reporting entity to identify and measure potentially higher risks and develop strategies to mitigate them so they can focus resources where they are most needed to manage risks within its own acceptable tolerance levels.
- Existing client identification, record keeping and reporting requirements still apply. The risk-based approach serves as an enhancement to those requirements.
- The risk-based approach will vary depending on the size and complexity of the reporting entity's operations.

# Risk-Based Approach: Requirements

- Assess and document, as appropriate for the reporting entity, the risk of money laundering or terrorist financing offences in the course of their activities.
- The risk assessment must take into account the reporting entity's:
  - clients
  - business relationships
  - products and services
  - delivery channels
  - geographic location of its activities and the location of its clients
  - other relevant factors related to the reporting entity's business

## Risk-Based Approach: Requirements (cont'd)

- For all activities that pose a **high** money laundering or terrorist financing risk, reporting entities must develop and apply policies and procedures to :
  - mitigate the identified risks of money laundering or terrorist financing offences;
  - take reasonable measures to keep client ID and beneficial owner information up to date every two years; and
  - take reasonable measures to conduct ongoing monitoring to detect suspicious transactions.

## Risk-Based Approach: Tools

- FINTRAC's Guideline 4 provides more information on:
  - Legislative and regulatory requirements;
  - Risk mitigation measures;
  - Suggestions on how to monitor;
  - Checklists which can be used as a starting point for developing a risk assessment by analyzing:
    - Products & services,
    - Delivery channels, geographical locations, and clients and business relationships.

# Administrative Monetary Penalty Regime

# Administrative Monetary Penalty (AMP) Regime

- Starting December 30, 2008, FINTRAC will be able to issue administrative monetary penalties as a response to non-compliance with the PCMLTFA and related regulations.

# Other Information

# FINTRAC's Compliance Approach

- FINTRAC is committed to a cooperative approach to compliance
- Continue to provide guidance on upcoming and existing requirements through the updating and development of FINTRAC guidelines

## For More Information

- Revised FINTRAC guidelines and other communications tools available
- Sector-specific presentations, webcasts and fact sheets available online
- Updates cover new requirements, most of which are effective June 23, 2008

## For More Information

Please consult FINTRAC's Web site:

[www.fintrac-canafe.gc.ca](http://www.fintrac-canafe.gc.ca)