

New PCMLTFA Obligations

Money Services Businesses

April 2008

Presentation Overview

- Introduction
- Objectives of New Requirements
- MSB Registration
- 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*
 - *Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations*
- Most 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 of a Money Services Business (MSB)

- Definition of MSB will include foreign exchange dealers
- An MSB means an individual or entity engaged in the business of any of the following activities:
 - foreign exchange dealing;
 - emitting or transmitting funds; or
 - issuing or redeeming money orders, travellers cheques or similar negotiable instruments except for cheques payable to a named individual or entity.

MSB Registration

- Effective June 23, 2008, all MSBs operating in Canada will have to be registered with FINTRAC.
- It will constitute an offence under the PCMLTFA to operate an unregistered money services business.

MSB Registration (cont'd)

- MSBs must renew their registration every two years.
- Must inform FINTRAC of changes or cessation of activities within 30 days.
- FINTRAC will act as registrar and can deny or revoke the registration.
- Registration is not a FINTRAC endorsement.

Registration Ineligibility Grounds

The following applicants are not eligible for registration:

1. Applicant is a listed person under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*.
2. Applicant is a listed entity under the *Criminal Code* terrorism provisions.
3. Applicant has been convicted of:
 - a money laundering or a terrorist activity financing offence;
 - a *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (on indictment);
 - a terrorism offence under the *Criminal Code*;
 - an organized crime offence under the *Criminal Code*;
 - a serious offence under the *Criminal Code* pertaining to fraudulent transactions (contracts and trade);
 - a serious offence under the *Controlled Drugs and Substances Act* (does not include simple possession).

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 you 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:
 - An international transfer of \$10,000 is cancelled because the client refuses to provide identification as requested by a teller.
- New information to be provided in STR form:
 - whether the transaction was completed
 - if not, the reason why it was not completed

EFT Beneficiary Information

- Rule #1: Reporting entity that is the initial recipient of an incoming international EFT of \$10,000 or more must report it.
- Rule #2 : In the context of a chain of transfers, reporting entities that are not the initial recipient of the international EFT of \$10,000 or more must also report if the message does not contain the beneficiary's name and address.

Bundled EFTs

- Effective since June 30, 2007
- The 24-hour rule does not apply in relation to EFTs sent to 2 or more beneficiaries where the transfer is requested by:
 - a public body or very large corporation (as defined in the regulations); or
 - an administrator of a pension fund regulated by a province or the federal government.

Changes to Client Identification and Record Keeping

Client Identification

- If client is present, refer to a valid government issued identification document
- Options for ascertaining client identity are expanded in non face to face situations (e.g. telephone, Internet services)

Client Identification: Non Face to Face Methods

1. Use of an affiliate

OR

2. Specific combinations of new 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

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); and
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 or credit file	AND	cleared cheque or confirmation of deposit account
attestation	AND	cleared cheque or confirmation of deposit account
attestation	AND	ID product or 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.

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.

Record Keeping

- As a result of the incorporation of foreign exchange dealers into the MSB definition:
 - An MSB that creates client credit files and internal memoranda about services provided to clients must keep them.
 - An MSB must also keep all transaction tickets in respect of a foreign currency transaction.

Remittance or transmission of \$1000 or more

- When you remit or transmit an amount of \$1000 or more (domestic or international), you must keep a record of:
 - If the client is an individual, their name, address, telephone number, date of birth, and nature of principal business or occupation
 - If client is an entity, the name, address, date of birth and telephone number of individual initiating transaction on behalf of entity and nature of that individual's principal business or occupation
 - Reference number and date of transaction
 - Name of individual to whom EFT is sent
 - Amount and currency of transaction
- And ascertain the identity of the client

Suspicious Transaction Report (STR)

- Reporting entities must keep copies of suspicious transaction reports (STRs) concerning both attempted and completed transactions.
- Reporting entities must take reasonable measures to ascertain the 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.

Ongoing Service Agreement with Entity

- Agreement for ongoing service to MSB clients that are corporations or other entities
- MSBs that enter into ongoing service agreement for the provision of MSB services shall confirm existence of the corporation or other entity and keep:
 - Name, address, date of birth and occupation of every individual who signed the agreement on behalf of entity,
 - Client information record with respect to the entity
 - A list containing name, address, date of birth of every employee authorized to order transactions
- Purpose: MSBs do not have to verify the identity of employees on the list that are placing transactions on behalf of an ongoing service agreement client

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 individual's 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 Owner: Record Keeping

For 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 entity other than 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 the 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

Politically Exposed Foreign Persons

- When a client initiates or receives an international EFT of \$100,000 or more, MSBs must take reasonable measures to determine if the client is a politically exposed foreign person (PEFP).
- The determination must be made within 14 days following the transaction.

Politically Exposed Foreign Persons (cont'd)

- 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.
- It 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, step-brother, step-sister)

PEFP: 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: Additional measures

- If a client is determined to be a PEFP, the following additional measures must be applied:
 - Take reasonable measures to establish source of funds.
 - Have senior management review transaction within 14 days of transaction.
- A **total** of 14 days for making determination **and** seeking review.

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 or transaction
- Awareness of the money laundering or terrorist financing risks to which the MSB or this type of transaction is exposed
- Awareness of politically exposed foreign persons

Politically Exposed Foreign Persons

- 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 reviewed transaction
 5. Date of review

EFTs: Originator Information & Travel Rule

EFTs: Originator Information and Travel Rule

- Requirements:
 - MSBs that **send** EFTs shall include with the transfer the full name, full address, account number or other reference number if any (originator information).
 - MSBs that **receive** EFTs must take reasonable measures to ensure that the message includes originator information.

EFTs: Originator Information and Travel Rule (cont'd)

- EFTs that are covered:
 - Domestic SWIFT MT 103 and all international EFTs (if SWIFT, only MT 103s) that are sent at the request of client
 - Does not apply to certain types of transfers e.g. credit or debit card transaction, etc.
- The travel rule applies unless the EFT is sent by a system that does not allow for the transfer of such information.
- However, all MSBs will have to comply by June 2009, regardless of system capabilities.

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 a by 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 your 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 Approach to Compliance

- 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

Key Events

- Revised FINTRAC guidelines and other communications tools: starting in February 2008
- Information sessions: February 2008
- Webinars: April and May 2008
- Most new provisions are effective June 23, 2008

For More Information

Please consult FINTRAC's Web site:

www.fintrac-canafe.gc.ca