

New PCMLTFA Obligations

Financial Entities

April 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

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:
 - A cash deposit 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 Record Keeping and Client Identification

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

EFTs of \$1000 or more

- When sending certain EFTs of \$1000 or more **at the request of a client:**
 - 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
 - Account number if any, reference number of transaction if any, and date of transaction
 - Name or account number of the individual or entity to whom EFT is sent
 - Amount and currency of transaction
- Requirement applies to International EFTs (for SWIFT EFTs only MT 103s) and domestic SWIFT MT 103s
- Must ascertain identity of individual if the signature card is not signed

Travellers' Cheques and other Instruments of \$3000 or more

- Receipt of \$3000 for travellers' cheques, money orders or other negotiable instruments:
 - Amount
 - Date received
 - Name and address of individual who gave amount
 - Whether amount received was in cash, cheques, traveller's cheques, money orders or other
- Must ascertain identity of individual, if signature card is not signed.

Redemption of Money Orders of \$3000 or more

- Redemption of one money order of \$3000 or more, or two or more money orders that add up to \$3000 or more:
 - Total amount
 - Date of redemption
 - Name and address of individual requesting redemption
 - Name of issuer(s)
- Must ascertain identity of individual, if signature card is not signed.

Intended Use of Account

- For every account opened, must have a record of its intended use.
- Examples of intended use for personal accounts include:
 - for general cheque services, such as payment of family and household expenses
 - to receive directly deposited employment or pension income
 - to save for retirement, and so on
- Examples of intended use for commercial accounts include:
 - for deposits of daily receipts for a business (i.e., sales, etc.)
 - for payments to employees (payroll)
 - for general business operating expenses, and so on

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.

Credit Card Accounts: Record Keeping

- When opening a credit card account for a **client that is an individual**:
 - Name
 - Address
 - Date of birth
 - Principal occupation or business
 - Name, address, telephone number of every credit card holder
 - Date of birth of every credit card holder, if possible
 - Every credit card application
 - Every credit card statement

Credit Card Accounts: Record Keeping (cont'd)

- When opening a credit card account in the name of a **corporation**:
 - Copy of the part of official corporate records containing power to bind
 - Name, address, telephone number of every credit card holder
 - Date of birth of every credit card holder (if possible)
 - Every credit card application
 - Every credit card statement

Credit Card Accounts: Record Keeping (cont'd)

- When opening a credit card account for an **entity other than a corporation**:
 - Name of entity
 - Address of entity
 - Principal business of that entity
 - Name, address and telephone number of every card holder
 - Date of birth of every card holders, if possible
 - Every credit card application
 - Every credit card statement

Credit Card Accounts: Client Identification

- A financial entity shall in the case of credit card accounts ascertain the identity of an individual in whose name the account is opened.
- Where the financial entity opens a credit card account in the name of a corporation it must confirm existence and ascertain name, address of the corporation and the names of all its directors.
- Where the financial entity opens a credit card account in the name of an entity other than a corporation, it must confirm existence of the entity.

Client Identification

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

New Rules:

- Options for ascertaining client identity are expanded in non face-to-face situations (e.g. telephone, Internet services)
- Prohibition to open account if unable to establish identity

Client Identification: Non Face-to-Face Methods

1. Use of an affiliate or co-member
OR
2. Specific combinations of new identification methods:
 - cleared cheque
 - identification product method
 - credit file method
 - attestation method
 - confirmation of a deposit account

Affiliate or Co-Member Method

- Method can be used by affiliates or co-members of an association.
- 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.
- The method can also be used by an entity that is a co-member of the same association (central or federation).

Affiliate or Co-Member 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)
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 Combination 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 Combination 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 (NFTF) Methodes for All

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

- Use an affiliate or co-member
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: NFTF for Credit Card Accounts - Option 1

Additional combinations of identification methods are available:

- Financial entities may combine any methods in either Part A or B of Sch. 7 of the PCMLTF Regulations, including:
 - Pairing information from the same source, i.e. cleared cheque and confirmation of deposit account or identification product and credit file
 - Using the independent data source method (reverse look-up)
- Identification must be ascertained before any credit card is issued on the account.

Client Identification: NFTF for Credit Card Accounts - Option 2

- When client has no credit history in Canada:
 - Financial entities may pair any methods in Part A, B or C of Sch. 7 of the PCMLTF Regulations which includes the following additional methods (only available for this Option 2):
 - Utility invoice, photocopy of ID, deposit account statement
- However, credit limit cannot exceed \$1500

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 and Client Identification Exemptions

- New exemptions have been added, for example:
 - If an entity is a subsidiary of a large corporation (minimum net assets of \$75 million) and has its financial statements consolidated with the large corporation.

Exemptions: Credit Card Acquiring Activities

- Financial entities that have credit card acquiring activities are exempted from record keeping and client identification requirements with respect to those activities.
- Financial entities that have credit card acquiring activities are however subject to STR obligations, must conduct a risk assessment and have compliance regime obligations.

Third Party Determination

- An employee depositing cash in an employer's **business** account is not considered to be acting on the behalf of a third party. Therefore no third party determination required.

Foreign Branches and Subsidiaries

Foreign Branches and Subsidiaries

- Financial 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.

New Due Diligence Measures

Correspondent Banking

- Effective since June 30, 2007
- New record keeping and due diligence measures when a financial entity enters into a correspondent banking relationship with a foreign financial institution
- For more information, please consult Guideline 6G for Financial Entities

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 politically exposed foreign person (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)

Politically Exposed Foreign Persons (cont'd)

Financial entities must take reasonable measures to determine if the client is a PEFP in the following situations:

- At account opening
- Based on risk assessment for existing accounts that are deemed high risk
- When a client is initiating or receiving an international EFT of \$100,000 or more

For new accounts, determination must be made within 14 days of account activation. For EFTs, determination must be made within 14 days of the transaction.

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 (cont'd)

- If a client is determined to be a PEFP, the following additional measures must be applied:
 - Take reasonable measures to obtain source of funds.
 - Must obtain senior management approval to maintain account or have senior management review transaction within 14 days of account activation or EFT transaction.
 - Must conduct ongoing monitoring of account to identify suspicious transactions.
- A **total** of 14 days for making determination **and** obtaining approval / 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 financial entity or this type of account or transaction is exposed
- Awareness of politically exposed foreign persons

Politically Exposed Foreign Persons: Record Keeping

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

EFTs: Originator Information and Travel Rule

EFTs: Originator Information and Travel Rule

- Requirements:
 - Financial entities that **send** EFTs shall include with the transfer the full name, full address, account number or other reference number if any (originator information).
 - Financial entities 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 financial entities 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,
 - approved by senior officer, and
 - kept up-to-date
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.
 - 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. 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** ML or TF 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 at least 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;
- FINTRAC will continue to provide guidance on upcoming and existing requirements through the updating and development of FINTRAC guidelines.

Key Dates

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

For More Information

Please consult FINTRAC's Web site:

www.fintrac-canafe.gc.ca