

New PCMLTFA Obligations

Casinos

April 2008

Presentation Overview

- Introduction
- Objectives of New Requirements
- Changes to Reporting
- Changes to Client Identification and Record Keeping
- 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:
 - Client would like to purchase chips with a large amount of cash (\$12,000) but refuses to provide identification as requested by the teller. Transaction is cancelled by teller.
- New information to be provided in STR form:
 - whether or not the transaction was completed
 - if not, the reason why it was not completed

Reporting of EFTs

- Casinos must report to FINTRAC:
 - EFTs of \$10,000 or more that are sent out of Canada at the request of a client
 - EFTs of \$10,000 or more that are received from outside of Canada at the request of a client

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.

Changes to Client Identification and Record Keeping

Client Identification

- If client is physically present, only identification method is to 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

- Use of specific combinations of identification methods:
 - identification product method
 - credit file method
 - attestation method
 - confirmation of a deposit account
 - cleared cheque

Client Identification: Non Face-to-Face Methods (cont'd)

- **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.

Client Identification- 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 (cont'd)

- In non-face-to-face situations, will be possible to use 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, reporting entities are 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 a 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: New Rules

- Keep transaction ticket for **every** foreign currency exchange
 - Amount, currency, date of purchase or sale, method of payment, amount and currency of payment made or received
- If foreign exchange is for \$3000 or more, name and address of the individual carrying out transaction must be recorded. Must also ascertain identity.

Record Keeping: New Rules (cont'd)

- When the casino remits or transmits an amount of \$1000 or more (domestic or international), 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
 - Account number if any, reference number, if any, and date of transaction
 - Name or account number of individual or entity to whom EFT is sent
 - Amount and currency of transaction
- Ascertain the identity of the client

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.

EFTs: Originator Information & Travel Rule

EFTs: Originator Information & Travel Rule

- Requirements:
 - Casinos that **send** EFTs shall include with the transfer the name, address, account number or other reference number if any (originator information)
 - Casinos 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 casinos 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 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, it 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. 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, and
 - other relevant factors related to its 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 a money laundering or terrorist financing offences;
 - take reasonable measures to keep client ID 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
- 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
- Webcasts: April 2008
- Most provisions are effective June 23, 2008

For More Information

Please consult FINTRAC's Web site:

www.fintrac-canafe.gc.ca