Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

Consultation Paper

June 2005

Canada

Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

Consultation Paper

June 2005

Department of Finance Canada
Ministère des Finances Canada

Copies of this document may be obtained from the:

Distribution Centre
Department of Finance Canada
Room P-135, West Tower
300 Laurier Avenue West
Ottawa, Ontario K1A 0G5
Telephone: (613) 995-2855
Facsimile: (613) 996-0518

Also available on the Internet at www.fin.gc.ca

Cette publication est également disponible en français.

Table of Contents

Preface

The purpose of this paper is to set out the Government of Canada's ("the Government") proposals to strengthen Canada's anti-money laundering (AML) and anti-terrorist financing (ATF) framework. These proposals reflect the Government's goal of being at the forefront in the global fight against these crimes, thereby contributing to public safety in Canada and worldwide. In addition, this paper is designed to meet several key domestic and international requirements, including:

- the need to meet Canada's international obligations as a member of the Financial Action Task Force (FATF) under its revised Forty Recommendations and Nine Special Recommendations to combat money laundering and terrorist financing. The FATF is the international standard setter in the area of AML and ATF;
- the need to address the recommendations of the Auditor General of Canada, as expressed in the *2004 Report of the Auditor General of Canada*, and the recommendations of the Treasury Board-mandated evaluation conducted by Ekos Research Associates;
- the need to address various stakeholder concerns, particularly those of law enforcement and intelligence agencies; and
- the need to review Canada's AML and ATF framework in preparation for the upcoming legislative review of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

Governments and international bodies such as the FATF are continuing to strengthen measures to deter global money laundering and terrorist financing operations. These international efforts have important implications for Canada and its commitment to maintain a world-class AML/ATF regime.

Proposals Relevant to Stakeholders

Stakeholder	Proposal Number
Financial entities (banks, credit unions and caisses populaires, and trust and loan companies)	1.4-1.13 2.1 3.2 5.1 6.1, 6.2, 6.5, 6.7, 6.8, 6.10-6.16
Crown corporations that take deposits	1.4, 1.5, 1.7, 1.8, 1.10, 1.11 2.1 3.2 5.1 6.5, 6.7, 6.8, 6.12-6.16
Life insurance companies, brokers and agents	1.4, 1.5, 1.7, 1.8, 1.10, 1.11 2.1 3.2 5.1 6.5, 6.8, 6.10-6.16
Securities dealers	1.4, 1.5, 1.7-1.13 2.1 3.2 5.1 6.1-6.3, 6.5, 6.7, 6.8, 6.11-6.16
Money service businesses	1.4, 1.5, 1.8-1.13 2.1 3.1, 3.2 5.1 6.1, 6.2, 6.5, 6.8, 6.11-6.16
Foreign exchange dealers	1.4, 1.5, 1.8-1.13 2.1 3.1, 3.2 5.1 6.1, 6.2, 6.5, 6.8, 6.11-6.16
Accountants and accounting firms	1.1, 1.3-1.5, 1.8, 1.10, 1.11 2.1 3.2 5.1 6.5, 6.8, 6.12-6.16

Stakeholder	Proposal Number
British Columbia notaries	1.1, 1.3-1.5, 1.8, 1.10. 1.11 2.1 2.5 3.1 5.1 6.5, 6.7, 6.8, 6.12-6.16
Real estate brokers, sales representatives or real estate developers	1.2-1.5, 1.8, 1.10, 1.11 2.1, 2.4 3.2 5.1 6.5, 6.8, 6.9, 6.12-6.16
Casinos	1.4, 1.5, 1.8, 1.10-1.13 2.1 3.2 5.1 6.1-6.8, 6.12-6.16
Dealers in precious metals and stones	1.4, 1.5, 1.8, 1.10, 1.11 2.3 3.2 5.1 6.5, 6.7, 6.8, 6.12-6.16
Legal counsel and legal firms	First section of Chapter 2
Importers/exporters of currency or monetary instruments	6.24, 6.25, 6.28, 6.30
Administrative provisions (do not affect reporting entities)	2.2, 4.1, 6.18-6.23, 6.26, 6.27, 6.29

The section "Issues for Further Consideration" at the end of Chapter 5 is of interest to:

- the white label automated teller machine (ATM) industry;
- financial entities;
- securities dealers;
- money service businesses;
- foreign exchange dealers; and
- casinos.

Introduction

The Government is committed to the fight against money laundering and terrorist financing. Money laundering is not only a serious threat to the integrity of the financial system, but it funds and creates incentives for further crime.

The regime is designed to provide appropriate tools to law enforcement to combat money laundering and terrorist financing while also respecting the personal privacy of Canadians and minimizing the compliance burden on reporting entities.

The potential damage to business and civil society of money laundering and terrorist financing necessitates a clear and effective strategy. This paper presents proposals on a series of critical measures that are required to update Canada's anti-money laundering (AML) and anti-terrorist financing (ATF) regime.

Canada's AML/ATF Regime

The core elements of Canada's AML regime were originally set out in the Proceeds of Crime (Money Laundering) Act (PCMLA) of 2000. In December 2001, following the passage of the Anti-terrorism Act (or "Bill C-36"), the scope of the PCMLA was expanded to include ATF measures and the Act was renamed the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

Part 1 of the PCMLTFA requires financial intermediaries to meet customer identification, due diligence and record-keeping standards and to report suspicious and prescribed transactions relevant to the identification of money laundering, terrorist financing and the possession of terrorist property. Part 2 of the Act is administered by the Canada Border Services Agency, and requires the reporting of the importation and exportation of cash or monetary instruments.

Part 3 of the PCMLTFA establishes the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). FINTRAC became operational in October 2001. Its primary functions are to receive reports under the PCMLTFA from reporting entities,[1] to analyze those reports for information relevant to money laundering and terrorist financing, and to provide key identifying information (e.g. account holder, transaction amount and date) to Canadian law enforcement agencies and other agencies such as the Canada Border Services Agency, the Canada Revenue Agency and the Canadian Security Intelligence Service in specific circumstances.

The PCMLTFA is subject to a parliamentary review, which is mandated to begin as early as July 2005.

---

[1] Reporting entities include banks, credit unions and caisses populaires, trust and loan companies, securities dealers, life insurance companies, brokers or agents, real estate brokers or sales representatives, accountants and/or accounting firms, money service businesses, foreign exchange dealers, casinos, and agents of the Crown that accept deposit liabilities or sell money orders.

Scope of the Review

Revised FATF Forty Recommendations

In 2003, the Financial Action Task Force (FATF), the inter-governmental body that sets international standards for AML and ATF policies, updated its Forty Recommendations to ensure that they remain timely and relevant to the evolving threat of money laundering and terrorist financing. The revised Recommendations introduce a number of key changes to a range of money laundering and terrorist financing measures, including:

- the adoption of a stronger standard for money laundering predicate offences;
- the extension of the customer due diligence process for financial institutions, as well as "enhanced" customer identification measures for high risk customers and transactions;
- the coverage of designated non-financial businesses and professions (e.g. accountants; casinos; dealers of precious metals and stones; lawyers; notaries and independent legal professionals; real estate agents; trust and company service providers);
- the inclusion of key institutional measures in AML systems; and
- the improvement of transparency of legal arrangements.[2]

FATF member countries, including Canada, are strongly committed to meeting these Recommendations. The mutual evaluation process is the primary instrument by which the FATF monitors progress made by member governments in implementing the revised Recommendations. In Canada's case, an "on-site visit" for a third mutual evaluation is scheduled for late 2006, and the results of the assessment are to be published in early 2007.

Report of the Auditor General of Canada

In 2004, the Auditor General of Canada conducted an audit of the National Initiatives to Combat Money Laundering (NICML), which assessed the production, dissemination and use of financial intelligence, current compliance requirements and systems, and the extent to which performance is measured and reported.[3] The Auditor General concluded that Canada has a comprehensive strategy against money laundering and terrorist financing, which is in broad conformity with international standards.

---

[2] FATF Annual Report, 2002-2003.

[3] *2004 Report of the Auditor General of Canada*.

However, the Auditor General also identified areas of potential improvement. She noted, for example, that restrictions on the type of information FINTRAC may include in its disclosures to law enforcement and intelligence agencies can, at times, limit their usefulness. As well, she recommended that communication and feedback between partners be improved and performance measurement for the overall Initiative be strengthened.

Many of the recommendations of the Auditor General were echoed by Ekos Research Associates, which conducted a Treasury Board-mandated evaluation of the NICML in late 2004.[4]

Objectives of the Review

The Government is committed to being at the forefront in the global fight against money laundering and terrorist financing and to maintaining a world-class AML and ATF regime. The domestic and international context, and the fact that we now have the benefit of five years of experience with Canada's AML/ATF framework, provides Canada with an excellent opportunity to conduct a comprehensive review and significant updating of Canada's AML/ATF framework. With this in mind, the Government has organized its proposals around the following key objectives:

- strengthening "know your client" standards;
- closing gaps in Canada's AML/ATF regime;
- increasing compliance, monitoring and enforcement;
- strengthening FINTRAC's intelligence function; and
- coordinating and assessing overall AML/ATF efforts.

Other amendments and issues for future consideration will also be proposed. The proposals will affect all reporting entities under the PCMLTFA, that is:

- financial entities (banks, credit unions and caisses populaires, trust and loan companies);
- Crown corporations that take deposits;
- life insurance companies, brokers or agents;
- securities dealers;
- money service businesses;
- foreign exchange dealers;

[4] This report can be found at: http://www.fin.gc.ca/toce/2005/nicml-incba_e.html.

- accountants and accounting firms;
- lawyers and notaries
- real estate brokers or sales representatives; and
- casinos.

The Government recognizes that the development of a strong AML and ATF framework must be pursued in a manner that does not place an undue burden on reporting entities, which are on the front lines of the fight against money laundering and terrorist financing. Consideration will be given to the potential compliance challenges that reporting entities could face as a result of the proposals contained in this paper and the timing of implementation. For those proposals that place additional obligations on reporting entities, FINTRAC will provide guidance to clarify compliance requirements.

The Government looks forward to receiving the comments of interested parties on these proposals.

Written comments should be forwarded by September 30, 2005 to:

Diane Lafleur
Director, Financial Sector Division
Department of Finance
140 O'Connor Street
Ottawa, Ontario, K1A 0G5

Written comments may also be sent by facsimile to (613) 943-8436 or via email to fcs-scf@fin.gc.ca.

Please note that in this consultation initiative, we offer to post your submission on the Department of Finance Canada website. Please clearly indicate in your communication whether or not you grant us permission to post your comments on our website. If you do not give explicit permission, we will not post.

If you do give permission, we need the following information:

- **your full name;**
- **name of the organization for which you speak (if applicable);**
- **your full mailing address, including postal code;**
- **your telephone number, including area code; and**
- **your e-mail address and fax number, if applicable.**

You should indicate by which method you prefer to be contacted and whether you prefer to communicate in French or English.

Chapter 1
Strengthening Canada's Client Due Diligence Standards

The FATF and other international bodies, such as the Basel Committee for Bank Supervision, have increasingly focused on the importance of ensuring that reporting entities have adequate controls and procedures in place so that they know their customers. "Customer due diligence" is the foundation of a strong and effective AML and ATF regime. Without this due diligence, reporting entities can become subject to reputational, operational and legal risks, which can result in significant financial costs.

In the last few years, the FATF has identified a number of areas where the potential money laundering or terrorist financing risks were not adequately addressed by the Forty Recommendations. Such areas include the corruption of public officials, correspondent banking relationships, and the lack of transparency in the ownership of corporate vehicles. Also, the FATF identified the need to clarify the customer due diligence procedures outlined in its standards.

As a result of substantial international work in this area, the June 2003 revision of the FATF Forty Recommendations includes key changes to its customer due diligence standards. The client identification and record-keeping requirements under the Canadian regime meet most of the requirements set out in the revised FATF Recommendations.

Many countries have recognized the implementation and compliance challenges associated with the FATF requirements and have issued appropriate guidance in this respect. Canada will take a similar approach.

Enhanced Client Identification and Record-Keeping Requirements for Professional Intermediaries

The term "professional intermediaries" refers to professionals such as accountants and real estate professionals who act as financial intermediaries by facilitating financial transactions. It is important that these professionals implement appropriate measures to address the risk of being used by criminals to launder money or finance terrorist activities.

Currently, accountants, real estate brokers and sales representatives are subject to Part 1 of the PCMLTFA when they act as financial intermediaries. Under the regulations, they are required to identify the client and keep records only when they receive $10,000 or more in cash. However, to be fully compliant with FATF Recommendations, further measures are required. The standard is outlined in FATF Recommendation 12.

FATF Recommendation 12

"The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in the following situations:…

b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate….

d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities…."

PROPOSAL 1.1

Accountants and Accounting Firms

The Government proposes to amend the PCMLTF Regulations to expand the client identification and record-keeping requirements applicable to accountants or accounting firms beyond large cash transactions. The requirement would also apply to any of the following activities on behalf of a client:

- receiving or paying funds;
- purchasing or selling securities, real properties or business assets or entities; or
- transferring funds or securities by any means.

PROPOSAL 1.2

Real Estate Brokers and Sales Representatives

The Government proposes to amend the PCMLTF Regulations to expand the client identification and record-keeping requirements applicable to real estate brokers or sales representatives beyond large cash transactions. The requirement would also apply to any of the following activities on behalf of a client in the course of a real estate transaction:

- receiving or paying funds;
- depositing or withdrawing funds; or
- transferring funds by any means

PROPOSAL 1.3

Customer Due Diligence and Record-Keeping Requirements for Professional Intermediaries

The Government proposes to amend the PCMLTF Regulations to require accountants, accounting firms and real estate brokers or sales representatives, when engaged in the activities listed in Proposals 1.1 and 1.2, to:

- verify the identity of the client by referring to a government-issued identity document; and
- take reasonable measures to obtain the name, address and principal business or occupation of any third party on whose behalf a transaction is carried out and beneficial owners of any entity involved, as well as their relationship to the originator of the transaction, as outlined in proposals 1.9, 1.10 and 1.11.

Suspicious Transactions and Doubtful Client Information

The effectiveness of a suspicious transaction reporting regime relies heavily on the accuracy of client information. With a mandatory reporting regime in place, criminal elements may attempt to circumvent the reporting by providing false or incomplete identifying information. Entities covered by the PCMLTFA should increase their scrutiny of client identification and put in place processes to mitigate this risk. FATF Recommendation 5 outlines this requirement.

FATF Recommendation 5

"…Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:…

- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data…."

PROPOSAL 1.4

The Government proposes to amend the PCMLTF Regulations to require reporting entities subject to Part 1 of the Act to take certain measures in the following situations:

- When there is a suspicion of money laundering or terrorist financing and the identity of the client has not previously been ascertained, the reporting entity should identify and verify the customer's information. In this situation, verification should be undertaken only to the extent that it can be accomplished without "tipping off" the customer about the suspicion.

- When there is a suspicion of money laundering or terrorist financing, and there are doubts about the veracity or adequacy of previously obtained customer information, the reporting entity should repeat the process of identifying and verifying the customer's information. In this situation, verification should be undertaken only to the extent that it can be accomplished without "tipping off" the customer about the suspicion.

Records of the sources of information and the methods of identification should be kept in both cases.

Politically Exposed Persons (PEPs)

The FATF defines PEPs as individuals who are or have been entrusted with prominent public functions such as Heads of State, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and important political party officials. While the FATF Recommendation focuses on foreign PEPs, countries are increasingly expanding the coverage of their regimes to both foreign and domestic PEPs, in line with the requirements of the United Nations Convention against Corruption and other international agreements.

There is international concern, particularly for some foreign jurisdictions, that PEPs constitute higher risk customers for financial institutions and intermediaries as they have potentially greater opportunities to engage in corrupt activities, and Canada will do its part in the global fight against corruption. To prevent the laundering of the proceeds of corruption, financial institutions and intermediaries should take additional steps to identify customers that are PEPs and apply enhanced due diligence measures.

FATF Recommendation 6

"Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.
b) Obtain senior management approval for establishing business relationships with such customers.
c) Take reasonable measures to establish the source of wealth and source of funds.
d) Conduct enhanced ongoing monitoring of the business relationship."

Article 52 of the United Nations Convention against Corruption

"…Each State Party shall take such measures as may be necessary, in accordance with its domestic law, to require financial institutions within its jurisdiction to verify the identity of customers, to take reasonable steps to determine the identity of beneficial owners of funds deposited into high-value accounts and to conduct enhanced scrutiny of accounts sought or maintained by or on behalf of individuals who are, or have been, entrusted with prominent public functions and their family members and close associates…."

PROPOSAL 1.5

The Government proposes to amend the PCMLTFA and regulations to require that for transactions above a certain threshold, when there are reasonable grounds to suspect that a new or existing customer is a foreign or domestic PEP, as defined under the regulations, reporting entities would have additional responsibilities. These entities would need to:

- have appropriate risk management systems in place to determine whether a customer is a politically exposed person;
- take reasonable measures to establish the source of funds;
- conduct enhanced ongoing monitoring of the business relationship; and
- obtain senior management approval to enact the transaction, open the account or continue the business relationship.

Correspondent Banking

Correspondent banking is the provision of banking services by a bank (the correspondent bank) to another bank (the respondent bank). To address the potential abuse of correspondent banking relationships by criminals, it is important that Canadian financial institutions obtain sufficient information from respondent foreign banks, and pay special attention to relationships with banks located in countries with weak customer due diligence standards. The FATF prescribes enhanced due diligence measures for cross-border correspondent banking and similar relationships in Recommendation 7.

FATF Recommendation 7

"Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.
b) Assess the respondent institution's anti-money laundering and terrorist financing controls.
c) Obtain approval from senior management before establishing new correspondent relationships.
d) Document the respective responsibilities of each institution.
e) With respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank."

PROPOSAL 1.6

The Government proposes to amend the PCMLTFA and regulations to require financial entities to take the following steps before entering into a correspondent banking relationship:

1. Obtain all relevant information on the activities and operations of the respondent bank, including its regulation and its anti-money laundering and anti-terrorist financing controls.
2. Obtain approval from senior management before establishing a new correspondent relationship.
3. Document the respective responsibilities of each institution.
4. Ensure that the respondent bank conducts appropriate due diligence and can provide relevant customer identification information for clients using "payable-through accounts."

The Government will also consider measures to prohibit financial entities from entering into or continuing a correspondent banking relationship with a shell bank, that is, a bank that has no physical presence in any country, or a respondent bank that permits its accounts to be used by a shell bank.

Lower Risk Situations

Although criminals can use a number of methods to launder money or finance terrorist activities, certain types of financial products present limited risks of being used for criminal purposes. The Government, and FATF Recommendation 5, recognize that it may not be necessary to impose client identification and record-keeping requirements in these situations.

FATF Recommendation 5

"…Financial institutions should apply each of the CDD [client due diligence] measures [under Recommendation 5]…, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures…."

PROPOSAL 1.7

- Amend the PCMLTF Regulations to exempt the following types of transactions from the client identification and record-keeping requirements:
  - the opening of an income trust reinvestment plan account sponsored by a fund manager for its investors, unless the account is funded in whole or in part by a source other than the fund manager;
  - the opening of a supplemental unemployment benefit plan account or a retirement compensation arrangement plan account unless the account is funded in whole or in part by contributions by a person or entity other than the employer;
  - the opening of an employee disability, dental, medical or benefit plan account governed under the Income Tax Act unless the account is funded in whole or in part by contributions by a person or entity other than the employer; or
  - accounts established for the holding of securities in trust pursuant to the escrow requirements of Canadian securities regulators.
- Extend the record-keeping exemptions to the range of transactions that are exempt from the client identification requirements under the current regulations.

Non-Face-to-Face Situations

New technologies and business models are continually being developed by the financial sector in order to respond to demands for faster, more flexible client service. These services include non-face-to-face transactions (NFFTs)—transactions and account openings where the customer cannot be physically present at any stage in the process.

These transactions, which may occur over the Internet or other interactive computer services, or over the telephone or other electronic data transmissions, are increasingly anonymous, creating a money laundering and terrorist financing risk.

To the extent possible, financial institutions and intermediaries should meet their customers in person and ascertain their identity by referring to a government-issued identity document. However, when this is not possible, customer identification measures should ensure that NFFTs can be conducted with the same confidence and surety as when a customer is physically present. The FATF and the Basel Committee paper *Customer Due Diligence for Banks* echo these concerns.

FATF Recommendation 8

"Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions."

FATF Recommendation 9

"Countries may permit financial institutions to rely on intermediaries or other third parties to perform…the CDD process or to introduce business….Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party…."

Basel Committee paper Customer Due Diligence for Banks

"In accepting business from non-face-to-face customers:

- banks should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview; and
- there must be specific and adequate measures to mitigate the higher risk."

PROPOSALS

When customer identity cannot be ascertained in person by the reporting entity, the Government proposes two options:

- relying on an agent or introducer; or
- using specific non-face-to-face customer identification measures.

PROPOSAL 1.8

Agents or Introducers

The Government proposes to amend the PCMLTF Regulations to allow any reporting entity to rely on another person or entity to ascertain the identity of their customer provided that the reporting entity has a contractual arrangement with the person or entity for the purpose of ascertaining customer identity. The agent would be required to ascertain customer identity in person be referring to a government-issued identity document as required under the regulations.

Under this provision, the reporting entity would have to obtain customer information from the person or entity ascertaining customer identity on its behalf and would be required to keep the records specified under the regulations. However, the ultimate responsibility for complying with the requirements would remain with the reporting entity.

PROPOSAL 1.9

Non-Face-to-Face Customer Identification Measures

The Government proposes to consult with reporting entities to establish appropriate non-face-to-face client identification requirements for financial entities, securities dealers, money service businesses and foreign exchange dealers. Such requirements would apply when the customer is not physically present at the time the client identification requirements are triggered (i.e. transactions conducted on the Internet, by phone or by mail) and identity cannot be ascertained in person by the reporting entity or an agent by referring to a government-issued identity document.

The appropriate measure or combination of measures would be based on the money laundering or terrorist financing risks associated with different types of financial services, and would ensure that customer identification is as reliable as in face-to-face situations. Baseline criteria have to be established in respect of client identification measures, whether documentary or not. Examples of such measures could include:

- confirming that a cheque drawn by the person on an account of a financial entity subject to the PCMLTFA has been cleared;
- confirming that the person's identity was ascertained by a financial entity as prescribed by the PCMLTF Regulations in a face-to-face situation; and
- verifying the customer's identifying information using an independent source such as a business information services company.

Identification of Third Parties and Beneficial Owners

In order to determine whether a business, non-profit organization or legal arrangement is being used to launder money or finance terrorism, it is necessary to understand their control and ownership structure. Practices or arrangements that provide anonymity of ownership and control can facilitate money laundering and terrorist financing, as well as complicate the seizure of the proceeds of crime during investigations.

The FATF recommends that financial institutions and intermediaries obtain adequate, accurate and timely information about the beneficial owners and control structures of their customers. Currently, under the PCMLTF Regulations, reporting entities are required to take reasonable measures to collect third party information when opening an account or conducting a large cash transaction.

In November 2004, the Government tabled legislation, the Canada Not-for-profit Corporations Act, to improve the financial accountability of non-profit organizations (NPOs), clarify the roles and responsibilities of directors and officers, and enhance and protect the rights of members. When it is passed, this legislation will increase transparency requirements for NPOs that are soliciting contributions from the public.

FATF Recommendation 5

"…The customer due diligence (CDD) measures to be taken are as follows:…

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows whom the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer…."

PROPOSAL 1.10

The Government proposes to amend the PCMLTF Regulations to require that, in every situation where customer identification requirements are triggered, reporting entities also obtain third party and beneficial owner information and take reasonable measures to verify this information.

- This requirement would not apply to situations that are explicitly exempt from the client identification requirements under the regulations.

Third Parties

- Reporting entities would be required to determine whether the customer is acting on behalf of a third party and obtain, verify and keep records of the name, address and occupation of all third parties, as well as their relationship to the customer.

Beneficial Owners

Corporations and Business Customers

- When the customer is a business, reporting entities would be required to obtain, verify and keep records of the name, address and occupation of all natural persons who own or control, directly or indirectly (for example through the ownership of a legal entity), more than 10 per cent of a corporation or partnership.

Non-Profit Organizations

- When the customer is an NPO, reporting entities would be required to obtain, verify and keep records of the name, address and occupation of all senior officers and directors.
- They would also be required to determine whether the NPO is soliciting, as defined under the Canada Not-for-profit Corporations Act, and keep a record of this information.

- They would also need to take reasonable measures to determine whether the NPO is a charity registered with the Canada Revenue Agency (CRA) and, if so, obtain and keep records of the CRA registration number and confirmation of the registration by referring to the CRA website or other means.

Trusts

- In respect of a trust, reporting entities would be required to obtain, verify and keep records of the name, address and occupation of all settlers and all living beneficiaries of the trust.
- Reporting entities would also be required to take reasonable measures to establish the source of funds.

Ongoing Due Diligence

Appropriate customer due diligence measures are not restricted to account openings or conducting certain transactions. An important part of this process is the ongoing monitoring of the business relationship to ensure that transactions remain consistent with the customer's profile. It is also essential that customer information be kept up-to-date. The FATF points to the importance of ongoing monitoring in Recommendation 5.

FATF Recommendation 5

"…The customer due diligence (CDD) measures to be taken are as follows:…

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds…."

PROPOSAL 1.11

The Government proposes to amend the PCMLTF Regulations to require that reporting entities:

- monitor their business relationships with their customers, including transactions, on an ongoing basis; and
- implement procedures to ensure that customer information remains up-to-date.

Electronic Funds Transfers Originator Information

Electronic funds transfers (EFTs) are a fast and efficient way to move money within and between countries. EFTs are widely used in the layering stage of money laundering and to move funds to finance terrorist activities. In their efforts to detect and prevent these activities, financial intelligence units (FIUs), law enforcement and intelligence agencies must be able to track the movements of criminal funds through EFT networks.

Of particular importance is information on the originators of EFTs included in EFT messages. It is essential to ensure that information on the originator of wire transfers is available to law enforcement and intelligence agencies to assist them in investigating and prosecuting money launderers and terrorists, to FIUs for their analysis of transaction reports, and to beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions. Accordingly, FATF Special Recommendation VII, outlined below, sets standards for the inclusion and retention of complete and accurate originator information in EFT messages. These standards apply to the ordering, intermediary and beneficiary financial institution.

The PCMLTF Regulations currently require financial entities, money service businesses and foreign exchange dealers to ascertain the identity of their clients and keep records for any EFT of $3,000 or more.

FATF Special Recommendation VII

"Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number)."

PROPOSAL 1.12

EFT Customer Due Diligence and Record-Keeping Requirements

The Government proposes to amend the PCMLTF Regulations to require that a financial entity, money service business, foreign exchange dealer, securities dealer or casino[5] initiating a domestic or international EFT at the request of a client, regardless of the amount, ascertain the identity of the client and keep records of the following information:

- name and address of the client;
- account number or reference number;
- telephone number of the client;
- name and address of the person on whose behalf the EFT is made;
- type and number of identity document; and
- name and address of the beneficiary.

PROPOSAL 1.13

Client Information Transmission

The Government proposes to amend the PCMLTFA to require that reporting entities conducting EFTs on behalf of their customers (i.e. financial entities, money service businesses, foreign exchange dealers, securities dealers and casinos) implement the following measures with respect to international EFTs:

- when initiating outgoing international EFTs, the reporting entity should include, at a minimum, the first two information elements above in the EFT message;
- when the reporting entity acts as an intermediary in the EFT payment chain, it should ensure that the above originator information remains with the EFT message; and
- when the reporting entity is the recipient of an EFT, it should take reasonable measures to ensure the EFT includes the above originator information.

[5] This requirement would only apply to securities dealers and casinos that have proprietary systems to affect wire transfers on behalf of their clients. Casinos and securities dealers would also be required to report international EFTs of $10,000 or more. Refer to proposal 6.3 for details.

Chapter 2
Closing the Gaps

Status of Negotiations With the Legal Profession

In November 2001, the Federation of Law Societies of Canada ("the Federation") launched a constitutional challenge on the application of the PCMLTFA and its regulations to the legal profession. In March 2003, the Government repealed the application of the PCMLTFA to the legal profession through regulatory amendments. At the same time, the Government indicated that it would develop a new legislative and regulatory regime for the legal profession that better takes into account the duties of legal counsel. Subsequently, the Attorney General of Canada reached an agreement with the Federation to adjourn the court case to November 2005. Most recently, the case was adjourned indefinitely pending re-initiation by any of the parties.

Since the FATF first commenced studying money laundering methods and techniques, lawyers have been consistently mentioned in its typology reports as being linked to money laundering schemes and cases. In June 2000, the FATF launched a review of its Forty Recommendations and decided to explore the role of lawyers and other professionals in money laundering schemes as a priority. In addition, the G8 and numerous domestic typologies involving lawyers point to the potential vulnerability of the profession to use by criminals. More recently, parliamentarians, the Auditor General and the media have identified the temporary exclusion of the legal profession as a significant gap in Canada's regime.

Since late 2003, the Department of Finance has been engaged in negotiations with the legal profession to develop a mutually acceptable regime.

Concurrently, the Federation endorsed a "model rule" prohibiting lawyers and legal firms from accepting more than $7,500 in cash in a single matter, with limited exceptions for monies received in respect of fees, disbursements, expenses or bail. Some provincial/territorial law societies have adopted the model rule in an effort to implement an industry alternative to suspicious and large cash transaction reporting. It is expected that each law society will implement these rules.

The Government will make a determination regarding the consistency and effectiveness of these rules and whether legislation or regulation is required with respect to large cash transactions. In addition, international standards, as set by the FATF, require that certain client identification, due diligence and record-keeping requirements for the legal profession be implemented through legislation or regulations. Discussions with the legal profession on each of these requirements are continuing and proposals will be forthcoming.

Reporting of Suspicious Attempted Transactions

Consistent with FATF standards, Canada's current anti-money laundering and anti-terrorist financing regime requires reporting entities to send to FINTRAC suspicious transaction reports, which contain designated information, when they have suspicions that a financial transaction relates to money laundering or terrorist financing. The general interpretation of this requirement has been that it applies only to transactions that have occurred. Nevertheless, some reporting entities voluntarily report suspicious attempted transactions to FINTRAC.

Other FATF member countries, such as Australia, the United Kingdom and the United States, require entities to routinely report suspicious attempted activities. International best practices demonstrate that there can be considerable analytical value in the information received from attempted transactions. Moreover, the analytical value of an attempted transaction report increases as more information about the transaction is provided.

The FATF, in its Interpretative Note, provides member countries with details on Recommendation 13. Specifically:

Interpretative Note to FATF Recommendation 13

"The reference to criminal activity in Recommendation 13 refers to:

a) all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction; or
b) at a minimum, to those offences that would constitute a predicate offence as required by Recommendation 1.

Countries are strongly encouraged to adopt alternative (a). All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.…"

PROPOSAL 2.1

The Government proposes to amend the PCMLTFA and its regulations to explicitly include the reporting of suspicious attempted transactions.

- All reporting entities that are currently obligated to report suspicious transactions under Part 1 of Act would be required to report suspicious attempted transactions.
- Guidance would be provided to reporting entities to assist them in determining when to report.

- The current form and manner of suspicious transaction reporting would remain unchanged except for the addition of information indicating that the transaction was not completed.
- At a minimum, reasonable efforts should be made to obtain the name and address of the individual undertaking the transaction and the amount of the transaction.
- The same record-keeping requirements in place for suspicious transactions would also apply to attempted suspicious transactions.

By requiring the mandatory reporting of such transactions, FINTRAC will be better able to comprehensively integrate this information into its analysis and improve the quality of its disclosures.

Information Sharing to Detect and Deter the Funding of Terrorism Through Registered Charities

International and domestic typologies indicate that non-profit organizations, such as charities, are vulnerable to abuse by terrorists as funding channels. These entities can be used in two ways. Terrorist groups can raise funds from willing or unwilling donors under the cover of a seemingly legitimate charity. Alternatively, they can infiltrate an existing charity, or create a new one, and divert the money of unsuspecting donors to fund acts of terrorism. Both of these methods would allow money generated by charitable fundraising activities in Canada to be sent abroad to support terrorist activities.

Since charities generally conduct transactions through financial institutions and intermediaries for their fundraising activities in Canada, they are subject to some degree of monitoring. For example, under the PCMLTFA, reporting entities are required to comply with client identification, record-keeping and reporting requirements that facilitate the detection of illicit activities involving customers that are charities. In addition, charities that seek a tax-exempt status and the authority to issue tax receipts to donors must register with the Canada Revenue Agency (CRA). As part of the registration and ongoing monitoring processes, the CRA reviews an organization's financial statements and can obtain information on its senior officers and directors.

However, a number of restrictions apply to the sharing of information on charities between the CRA and other agencies involved in the detection of terrorist financing. In particular, the Income Tax Act limits the circumstances under which the CRA can disclose its suspicions about the activities of specific organizations. Such disclosures can only be made for purposes of the CRA's administration and enforcement of the Charities Registration (Security Information) Act. Consequently, such information cannot be used by these investigative agencies to assist in their own counter-terrorism investigations. Also, the PCMLTFA does not allow FINTRAC to disclose information to the CRA on suspected terrorist financing cases involving charities.

FATF Special Recommendation VIII

"Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused" by terrorists.

FATF, Combating the Abuse of Non-Profit Organisations—International Best Practices

"Jurisdictions which collect financial information on charities for the purposes of tax deductions should encourage the sharing of such information with government bodies involved in the combating of terrorism (including FIUs) to the maximum extent possible. Though such tax-related information may be sensitive, authorities should ensure that information relevant to the misuse of non-profit organisations by terrorist groups or supporters is shared as appropriate."

PROPOSAL 2.2

The Government will review the Income Tax Act with a view to determining what mechanisms the CRA can employ in cases where there is evidence that a charity is being used or will be used for money laundering or terrorist financing activities. The disclosure of information on specific charities would be made to FINTRAC and law enforcement and intelligence agencies, for the application of specific anti-terrorist legislation.

- The provision would apply in respect of entities that are seeking registration with the CRA, that have been denied or that are already registered.
- The information disclosed would be limited to:
  - identifying information about the charity and its senior officials and directors;
  - information provided as part of the CRA's file on the charity, including information provided by the charity itself during the application and/or reporting processes, information obtained by the CRA from third party (open) sources in the course of its administration of the Income Tax Act and the Charities Registration (Security Information) Act; and
  - an explanation of the grounds for suspicion.

The Government also proposes to amend the PCMLTFA to allow FINTRAC to disclose information to the CRA when there are reasonable grounds to suspect that a registered charity is being used to fund terrorism. FINTRAC would first be required to determine whether the disclosure threshold for terrorist activity financing is reached.

- These disclosures would be subject to the same restrictions that currently apply to information disclosed to law enforcement and intelligence agencies. FINTRAC is only allowed to disclose specific information when it has reasonable grounds to suspect that the information would be relevant to a money laundering or terrorist financing investigation.

Dealers in Precious Metals and Stones (DPMSs)

Precious metals, stones and jewellery can present significant money laundering or terrorist financing risks as they have high value and are easy to conceal, and their origin is often difficult to determine. According to the FATF, precious metals and stones are used internationally as both a source of illegal funds to be laundered, as well as a mechanism for money laundering and terrorist financing.

Police investigations indicate that organized crime groups are taking a growing interest in Canada's expanding diamond industry. Unless preventative measures are taken, law enforcement authorities predict that the incidence of money laundering and terrorist activity financing in the sector will significantly increase in the future with the domestic expansion of the precious metals and jewellery industries. Internationally, the FATF, in response to cases in a number of countries, has revised its standards to included DPMSs in Recommendations 12 and 16.

FATF Recommendation 12

"The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in the following situations:…

c) Dealers in precious metals and dealers in precious stones - when they engage in any cash transaction with a customer equal to or above the applicable designated threshold…."

FATF Recommendation 16

"The requirements set out in Recommendations 13 to 15, and 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:…

b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold…."

PROPOSAL 2.3

The Government proposes to subject to the PCMLTFA persons or entities in the business of selling or purchasing gold, diamonds and other precious stones, including jewelry. The Government is seeking views from the industry on the following elements:

- segments of the industry that would be subject to the requirements (e.g. cutting, polishing, manufacturing, wholesale, retail);
- reporting of large cash and suspicious transactions;
- the range of client identification and record-keeping requirements that would be applicable; and
- compliance mechanisms.

Real Estate Developers

The requirements under Part 1 of the Act currently apply to real estate agents that are registered or licensed under provincial legislation in respect of the sale or purchase of real estate. However, the money laundering risk associated with the real estate sector also exists in respect of the sale of new homes and buildings. Real estate developers who sell directly to the public, but are not registered or licensed agents, undertake the same activities as those currently covered by the Act and, as such, should implement anti-money laundering measures.

PROPOSAL 2.4

The Government proposes to expand the definition of "real estate broker or sales representative" under the PCMLTF Regulations to include real estate developers. The amendments would subject this sector to the same client identification, record-keeping and reporting requirements as real estate agents. They would also be subject to the requirements proposed in Chapter 1 of this paper.

The proposed amendment would create a level playing field in respect of the application of the PCMLTFA to the real estate industry.

Notaries in British Columbia

Notaries in British Columbia engage in many of the same activities as other professionals already covered by the PCMLTFA. In particular, they:

- facilitate the buying and selling of real estate; and
- hold trust accounts for clients.

In carrying out these activities, they act as financial intermediaries, that is they receive and disburse funds for clients. As with other professionals, already covered by the Act, notaries in British Columbia are at risk of being abused by criminals to facilitate money laundering and terrorist financing by virtue of the services they offer. This is particularly true in the case of real estate transactions.

PROPOSAL 2.5

The Government proposes to include notaries in British Columbia as reporting entities under the PCMLTFA.

- These notaries would be subject to the same requirements for suspicious and large cash transaction reporting, client identification, record-keeping and internal compliance as other professionals. They would also be subject to the requirements proposed in Chapter 1 of this paper when they engage in any of the following activities on behalf of another person or entity:
  - receiving or paying funds;
  - purchasing or selling securities, real properties or business assets or entities; or
  - transferring funds or securities by any means.

By including notaries in British Columbia in the PCMLTFA, the Government is closing a gap in the coverage of the current regime and creating a level playing field for entities conducting similar transactions on behalf of clients.

Chapter 3
Improving Compliance Monitoring and Enforcement

Money Service Business (MSB) Registration

The MSB sector is diverse, ranging from large multinational firms to individuals operating in relative obscurity. However, the absence of licensing or registration in Canada makes the sector highly attractive to criminals looking for alternatives to the regulated banking sector to launder money or finance terrorism.

The PCMLTFA currently requires persons or entities engaged in the business of remitting funds, providing foreign exchange services, or issuing or redeeming money orders, traveller's cheques or other negotiable instruments to abide by reporting, client identification, record-keeping and internal compliance requirements. However, unlike the other reporting entities covered by the Act, there is no framework requiring the licensing or registration of MSBs and foreign exchange dealers, and therefore limited means for FINTRAC to identify these entities and implement a risk-based compliance regime.

FATF Special Recommendation VI requires that countries take measures to ensure that money service businesses are subject to registration or licensing.

FATF Special Recommendation VI

"Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions."

Internationally, regulation of the MSB and foreign exchange sector is varied. In the United States, money service businesses are subject to state-level licensing requirements and federal registration through the Financial Crimes Enforcement Network—FinCEN (the US financial intelligence unit), while HM Revenue & Customs is responsible for registering MSBs in the United Kingdom. Other jurisdictions, such as Japan and France, prohibit the operation of money service businesses and require that the activities of these entities be conducted through the regulated banking sector.

In Canada, some provinces (New Brunswick, Newfoundland and Labrador, Nova Scotia, Quebec and Saskatchewan) have implemented provincial licensing regimes for the payday loan sector. However, these regimes are intended to primarily support consumer protection objectives.

PROPOSAL 3.1

The Government proposes to amend the PCMLTFA and its regulations to establish a registration regime for MSBs and foreign exchange dealers for the purposes of anti-money laundering and anti-terrorist financing measures.

Entities Required to Register

- The regime would require MSBs and foreign exchange dealers, as currently defined in the PCMLTF Regulations, to register their operations. This would include persons or entities:
  - engaged in the business of remitting or transferring funds by any means;
  - engaged in the business of foreign exchange; or
  - issuing or redeeming money orders, traveller's cheques or other similar instruments.
- Certain exemptions to the registration requirement would be granted for entities already supervised under the regime, such as regulated financial institutions that provide money services.

Registrar

- FINTRAC would function as the registrar and be granted the power to collect certain information in respect of registration. The information collected would be used for the purpose of ensuring compliance with Part 1 of the PCMLTFA and regulations. The specific information to be collected would be outlined in regulations.

Registration Information

- Certain elements of registration information would be made public. Information publicly available could include basic information about the business and its location, such as name, address and telephone number of the entity or owner.
- Non-public information would be used to assess compliance risk and would be protected under the PCMLTFA. Examples of this information could include business volume, countries to which money is remitted and from which it is received, and bank account numbers.
- Applicants would be required to register electronically if they are capable of doing so. On completion of registration, the registrar would issue applicants a confirmation of registration.
- Consideration may be given to applying a registration fee upon registration and annual renewal fees thereafter.
- Registration for the purposes of the PCMLTFA would not constitute government certification, endorsement or regulation.

Sanctions for Non-Compliance

- Part 5 of the Act would be amended to make it a criminal offence to operate an unregistered money service business.

The proposed registration regime would reinforce FINTRAC's existing compliance function and meet international standards, and would also facilitate law enforcement's ability to identify non-compliant operators. The proposal does not aim to regulate the sector and does not constitute a licensing requirement.

Creating an Administrative and Monetary Penalties Regime

In addition to a strong anti-money laundering and anti-terrorist financing legislative and regulatory framework, it is important to establish a compliance regime with the capacity to impose appropriate penalties and sanctions on individuals and entities that are non-compliant with the PCMLTFA and its regulations. This is consistent with FATF Recommendation 17.

FATF Recommendation 17

"Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by…[the FATF Forty Recommendations] that fail to comply with anti-money laundering or terrorist financing requirements."

In recent years, FINTRAC has entered into compliance-related information sharing relationships with federal and provincial financial services regulators for the monitoring of regulated institutions such as banks, insurance companies and securities dealers. These regulatory agencies have a range of tools to ensure compliance. FINTRAC's experience has shown that the unregulated sector, which includes entities such as money service businesses and foreign exchange dealers, poses special compliance challenges. A range of tools is required to enhance compliance in the regulated and unregulated sectors.

Under the PCMLTFA, FINTRAC has the option of referring cases to law enforcement. This can lead to criminal penalties of up to $2 million in fines and five years in prison for non-compliance. FINTRAC also makes use of various outreach and education programs to promote compliance. However, a broader range of non-criminal sanctions would clearly provide greater flexibility for FINTRAC in ensuring compliance with the PCMLTFA and its regulations.

International best practices suggest that administrative and monetary penalties (AMPs) provide scope for a more graduated approach. AMPs include an array of measures such as warning letters, tickets, permit cancellations and monetary fines. The flexibility offered by this range of options provides useful tools for enhancing compliance with the law through the PCMLTFA and its regulations.

A number of existing federal regulatory schemes have successfully employed AMPs to promote compliance with statutory requirements. For example, AMPs have been assessed for violations relating to income tax, employment insurance and customs. More recently, AMPs have been imposed by the Financial Consumer Agency of Canada as an effective means of ensuring compliance with the consumer protection provisions in financial institutions statutes. As well, the Office of the Superintendent of Financial Institutions is currently in the process of implementing an AMP regime for federally regulated financial institutions.

In regards to AML/ATF statutes, the Financial Services Authority (FSA) in the United Kingdom and FinCEN in the United States make use of AMPs for violations of the reporting, record-keeping or other requirements of their respective AML/ATF laws.

PROPOSAL 3.2

The Government proposes to create an AMP regime to deal with individuals and entities that do not comply with the requirements of the PCMLTFA. The key features of this regime would include:

- a clear description of the violations under the PCMLTFA and associated regulations to be dealt with through the use of AMPs. These violations would include failure to:
  - identify clients and keep appropriate records;
  - report suspicious transactions, large cash transactions, electronic funds transfers and terrorist property;
  - implement an appropriate compliance regime, including the appointment of a designated compliance officer and the establishment of appropriate policies, procedures and training programs for employees.
  - provide accurate, timely and complete reports and information to FINTRAC; and
  - cooperate with a FINTRAC compliance officer.
- a clear schedule of graduated penalty amounts would be established following appropriate consultations with reporting entity stakeholders.
- penalties would be established in regulations and would be assessed by FINTRAC in accordance with clearly established criteria.
- a Notice would be issued to entities that do not comply, which identifies the nature of the violation and the amount of the penalty.
- the Notice would review the range of options available to the offender, including the right to appeal and the recourse to a defence of due diligence; and
- the name of the offender and details of the violation would be made available on FINTRAC's website.

- AMPs would be used as a complementary compliance tool to criminal sanctions, which will continue to be available to deal with the most severe violations (e.g. wilful non-compliance). The capacity to impose an array of AMPs when persons or entities demonstrate non-compliance with AML/ATF laws will enhance FINTRAC's overall compliance program.

Sharing Compliance-Related Information With Foreign Partners

Currently, the PCMLTFA does not allow FINTRAC to exchange compliance-related information with its foreign counterparts. The legislation limits FINTRAC to the exchange of information for investigation and prosecution purposes. As many reporting entities operate across international borders, greater cooperation with FIUs and regulators abroad would ensure more comprehensive compliance assessments.

Sharing compliance-related information also has the advantage of facilitating multilateral coordination of simultaneous audits of specific reporting entities and supporting more robust international cooperation.

PROPOSAL 3.3

The Government proposes to establish legislative authority to allow FINTRAC to share compliance-related information with foreign entities that have similar compliance functions.

- A Memorandum of Understanding (MOU) between FINTRAC and its foreign counterparts with similar compliance functions would be used to outline the terms and conditions for sharing compliance-related information.
- The MOU would identify the parties to the agreement, the type of information eligible for exchange, limits on the use of the information and restrictions on third party dissemination of the information.
- Examples of the type of compliance information which would be eligible for sharing include:
  - case-specific information on compliance deficiencies;
  - examination results; and
  - risk assessment information.

Allowing for the controlled exchange of compliance-related information would assist FINTRAC in bolstering its compliance function by providing it with enhanced access to information from its foreign partners, which in turn serves to improve its ability to supervise compliance of Canadian reporting entities.

Chapter 4
Strengthening FINTRAC's Ability to Provide Intelligence

Expanding the Information Contained in FINTRAC Disclosures

The PCMLTFA allows FINTRAC to disclose certain information to law enforcement when it has reasonable grounds to suspect that the information would be relevant to investigating money laundering or terrorist financing. FINTRAC can also disclose information to the Canadian Security Intelligence Service (CSIS) where there are reasonable grounds to believe that this information would be relevant to the security of Canada. Under the PCMLTFA and its regulations, this information includes the date and place of a transaction, its value, and the names and associated account numbers of the parties involved.

When a FINTRAC disclosure is related to an ongoing investigation, it contributes useful information by providing new facts or leads for investigators. However, the information contained in FINTRAC disclosures is often perceived by law enforcement recipients as being too limited to warrant initiating a new investigation. This was one of the key findings of the Auditor General's 2004 report. Both the Auditor General and a Treasury Board-mandated evaluation of the regime in 2004 have recommended that an assessment be undertaken to consider changes that could be made to improve the value of FINTRAC disclosures.

International experience suggests that other financial intelligence units generally provide their law enforcement and intelligence agencies with more information relating to suspected financial transactions.

Auditor General of Canada Recommendation

"The Government should carry out a review to identify changes that would improve the value of FINTRAC disclosures and the means to bring about those changes." (*2004 Report of the Auditor General of Canada*)

Ekos Research Associates Recommendation

"It is recommended that the Government of Canada assess the feasibility of increasing the amount of information that may be included in FINTRAC disclosures in order to improve their value to disclosure recipients." (*Year Five Evaluation of the National Initiatives to Combat Money Laundering and Interim Evaluation of Measures to Combat Terrorist Financing*)

Under the PCMLTFA, law enforcement and intelligence agencies that want more information from FINTRAC can apply to the courts for a production order to access additional details on transactions and the analysis supporting the disclosure. However, law enforcement has generally been reluctant to pursue production orders because they must satisfy the court that there are reasonable grounds to believe an offence has been committed.

PROPOSAL 4.1

The Government proposes to expand the current list of designated information that FINTRAC can disclose to law enforcement and intelligence agencies to also include:

- additional publicly available information (including information from commercially available databases), such as:
  - telephone numbers;
  - names of related parties (e.g. partners or company directors); and
  - background information obtained from open sources (e.g. media articles).
- additional account information (e.g. type of account);
- Canada Revenue Agency-issued business numbers;
- the type of transaction (e.g. asset or good purchased);
- the type of report (e.g. suspicious transaction report) from which the information disclosed is compiled; and
- the reasons for suspicion.

The objective of expanding the information available in FINTRAC disclosures is to enhance the critical identifiers and investigative links that law enforcement and intelligence agencies can use to further money laundering and terrorist financing investigations while respecting the privacy and Charter rights of Canadians.

Chapter 5
Coordinating and Assessing AML/ATF Efforts

Creating a New AML/ATF Advisory Committee

Cooperation among federal departments and agencies, provincial and municipal law enforcement agencies, regulatory authorities, financial sector participants, and other reporting entities is critical to the success of Canada's initiative to combat money laundering and terrorist financing. As stated in the *2004 Report of the Auditor General of Canada*, more effective mechanisms are needed for coordinating efforts both within the federal government and among all stakeholders. Specifically:

Auditor General of Canada Recommendation

"The Government should establish an effective management framework to provide direction and co-ordinate anti-money-laundering efforts at the federal level. It should also consider establishing an anti-money-laundering advisory committee with representatives of government, industry, and law enforcement to regularly discuss issues of common interest and develop approaches for dealing with emerging issues." (*2004 Report of the Auditor General of Canada*)

The federal departments and agencies that are involved in Canada's anti-money laundering and anti-terrorist financing initiative interact regularly with each other and with external stakeholders. For example, the Department of Finance chairs regular interdepartmental meetings of its partners (at both working and managerial levels) to develop domestic policy and to identify operational issues. This management framework aims to provide direction and coordination of anti-money laundering and anti-terrorist financing efforts at the federal level. In addition, FINTRAC has various outreach programs to private sector stakeholders and consults extensively with law enforcement and intelligence agencies. The Department of Finance, as the policy lead, also consults with a wide range of industry stakeholders.

While these fora have been successful in coordinating initiative-wide efforts, the Government is committed to a constructive review of current mechanisms. To improve its management framework, the Government has reviewed international best practices and recommends the establishment of a formal advisory committee for the overall initiative that would bring representations from government, industry and law enforcement together in a single forum.

The Auditor General has noted that the United Kingdom and the United States have established anti-money laundering advisory committees with representatives of law enforcement, government and industry. These committees meet twice a year to consider emerging issues and to develop coordinated strategies to address them. They have proved useful in those countries, and we believe that such committees could play a constructive role in Canada.

The UK and US advisory committee models differ in their design and approach. The UK Money Laundering Advisory Committee is an informal body that focuses on policy issues and serves as a general forum for broad consultations. It consists of about 25 members. In contrast, the US Bank Secrecy Act Advisory Group is a legislated mechanism with a broad mandate that has many of the characteristics of a decision-making body. It is a group of about 45 members.

Although they differ in their mandates and approach, both the UK and US models highlight that an overarching advisory committee with broad representation allows for various stakeholders, particularly the private sector, to become more engaged with the process. As well, it offers an opportunity for the FIUs, law enforcement and intelligence agencies to provide valuable feedback to the private sector.

PROPOSAL 5.1

To support the management framework of Canada's anti-money laundering and anti-terrorist financing regime, the Government proposes that an AML/ATF advisory committee be established. The committee would have the following key characteristics:

- the committee's mandate would be to advise the Government on issues of common interest and develop approaches for dealing with emerging issues;
- the committee would serve as a discussion forum among various public sector and private sector stakeholders in Canada;
- the committee would comprise about 20-25 senior representatives from the public and private sectors;
- private sector representatives would include the Canadian banks and other deposit-taking institutions, insurance companies, securities dealers, money service businesses, and other affected sectors;
- the committee would meet twice a year (or more frequently if necessary), with the option of using a working group structure to examine selected issues in greater detail; and
- the committee would be chaired by the Department of Finance.

Consistent with the recommendation of the Auditor General, the Government believes that the creation of such an advisory committee would lead to effective coordination of AML/ATF efforts at the federal level.

Parliamentary Review of the PCMLTFA

Currently, provisions in the PCMLTFA require the administration and operation of the Act to be reviewed by Parliament five years after coming into force. Five years have passed since Bill C-22 (i.e. the original PCMLA) came into force and, as such, Parliament will begin reviewing the provisions of the PCMLTFA.

PROPOSAL 5.2

Given the evolving nature of criminality and money laundering/terrorist financing-related offences, it is important that Canada maintain an AML and ATF regime that is effective and up-to-date. Therefore, the Government proposes to renew the parliamentary review provision so that the Act may be reviewed by Parliament five years after the coming into force of a new AML and ATF scheme. This will allow the Government to assess the results and performance of the AML and ATF regime and to make timely improvements to the legislation and associated regulations.

Issues for Further Consideration

Criminals are constantly seeking new and innovative avenues to conceal and move their funds. They often take advantage of emerging technologies and expand their activities to different sectors of the economy. Consequently, in addition to the specific proposals outlined in this paper, the Government will be reviewing the anti-money laundering and anti-terrorist financing regime in a number of areas. They include:

- working with law enforcement and the industry to address the potential money laundering risks associated with "white label" ATMs (i.e. machines that are not owned or operated by banks). The concerns with these ATMs arise from the possibility for owners or operators to self-load the machine with cash;
- reducing the $10,000 threshold for international EFT reporting; and
- reviewing the PCMLTFA requirements as they apply to financial services that are provided via the Internet.

Chapter 6
Other Proposals

In addition to the proposals outlined in the preceding chapters, the Government is proposing a number of other related amendments to the PCMLTFA and regulations. These are grouped in four categories: Part 1 requirements, compliance issues, FINTRAC disclosures and cross-border currency reporting.

Part 1 – Requirements

6.1 Bundled Electronic Funds Transfers

Reference: PCMLTF Regulations, section 3

Amendment

Clarify the reporting requirements in respect of bundled EFTs

Explanation

Under the regulations, two or more EFTs sent on behalf of the same customer in a 24-hour period and that total $10,000 or more must be reported to FINTRAC. Currently, when an EFT message contains instructions in respect of a transfer from a single customer to several beneficiaries (bundled EFT), it would be reportable as a single transaction if the aggregate amount exceeds $10,000. The proposed amendment would clarify that such EFTs are not reportable as one transaction, but rather any EFT in the bundle is reportable on an individual basis if it exceeds $10,000. The provision would apply in respect of institutional and commercial transactions such as salary and pension payments.

6.2 Beneficiary Information in EFTs

Reference: PCMLTF Regulations, section 28

Amendment

Establish a provision ensuring the reporting of beneficiary information in EFTs.

Explanation

EFTs entering Canada may be handled by one or more reporting entities before they reach the ultimate beneficiary. Under the current regulations, an incoming international EFT must be reported by the first reporting entity to process it as it enters Canada. As such, that entity may not have all the information on the customer who is the ultimate beneficiary. Under the proposed amendment, if the name and address of the beneficiary is not provided in the EFT message, the reporting entity that is the ultimate recipient of an international EFT would be required to report the EFT even if it is not the first reporting entity to handle the EFT as it enters Canada. The proposed amendment, which mirrors a similar provision on outgoing EFTs, would ensure that FINTRAC receives the beneficiary information.

6.3 Reporting of EFTs by Securities Dealers and Casinos

Reference: PCMLTF Regulations, sections 21 and 40

Amendment

Require securities dealers and casinos to report international EFTs of $10,000 or more to FINTRAC.

Explanation

Under the current regulations, financial entities, money service businesses and foreign exchange dealers are required to report large international EFTs. The proposed amendment would make the requirement more consistent across sectors since some securities dealers and casinos provide EFT services to their customers.

6.4 Large Disbursements by Casinos

Reference: PCMLTF Regulations, section 42

Amendment

Require casinos to report to FINTRAC any payment to a customer of $10,000 or more.

Explanation

Under the current regulations, casinos are required to ascertain the identity of the customer and keep a record when they disburse $10,000 or more in cash. The proposed amendment would extend this requirement to any payment to a customer, in cash, by cheque or any other means, of $10,000 or more, and would require casinos to report these transactions to FINTRAC.

6.5 Canada Revenue Agency-Issued Business Numbers

Reference: PCMLTF Regulations, schedules 1 to 6

Amendment

Require reporting entities to obtain and report business numbers.

Explanation

When ascertaining the identity of a customer that is a business, the proposed amendments would require reporting entities to obtain its CRA-issued business number. It would also require the business number to be reported to FINTRAC on a suspicious or prescribed transaction report.

6.6 Record-Keeping Threshold

Reference: PCMLTF Regulations, section 43

Amendment

Remove the $3,000 regulatory threshold in the regulations for the requirement that casinos keep foreign currency transaction tickets.

Explanation

Currently, casinos are required to keep foreign currency transaction tickets for transactions of $3,000 or more. All other entities required by the regulations to keep foreign currency transaction tickets must keep all tickets regardless of the amount. The proposed amendment would ensure consistency of the requirements across sectors.

6.7 Third Party Determination Requirement for Business Account

Reference: PCMLTF Regulations, section 7

Amendment

Clarify that the exemption from the third party determination requirement when an employee deposits cash in their employer's account applies only in respect of a business account.

Explanation

Under the regulations, an employee depositing cash in an employer's account is exempt from third party determination requirements. The proposed amendment would clarify that the exemption applies only in respect of cash deposited in the employer's business account and not an employer's personal account.

6.8 Terrorist Property Reports

Reference: PCMLTFA, section 7.1

Amendment

Require reporting entities to report to FINTRAC terrorist assets frozen under the United Nations Suppression of Terrorism Regulations and other related statutes.

Explanation

Currently, reporting entities are required, in addition to reporting to the RCMP and CSIS, to report to FINTRAC when they are in the possession of assets of a terrorist entity listed under the Criminal Code. The proposed amendment would require them to report to FINTRAC in respect of the assets of terrorists listed under the United Nations Suppression of Terrorism Regulations and other related statutes.

6.9 Property Managers

Reference: PCMLTF Regulations, section 37

Amendment

Exempt the activities of property managers from the obligations of real estate agents under Part 1 of the Act.

Explanation

Currently, some property managers have obligations under the PCMLTFA as they are required to hold a real estate licence to conduct property management activities in their province of operation. The proposed amendment would exempt transactions conducted in the course of property management activities from the application of Part 1 of the Act.

6.10 Application to Foreign Branches

Reference: PCMLTFA, section 5

Amendment

Clarify that Part 1 of the Act applies to branches of financial entities and insurance companies located outside Canada.

Explanation

Reporting entities such as banks and insurance companies have branches outside Canada. The amendment would clarify that reporting requirements under Part 1 apply to the extent that local laws and regulations permit, while client identification, record-keeping and compliance requirements apply in all cases.

6.11 Agents of Foreign Entities

Reference: PCMLTFA, section 5

Amendment

Require local agents of a parent company located outside of Canada to have all the obligations of parent companies located within Canada.

Explanation

Currently, reporting entities that act as agents for "parent" entities are only responsible for filing suspicious transaction reports and terrorist property reports with FINTRAC. All other obligations reside with the parent entity. However, the requirements of the PCMLTFA are difficult to apply to the parent entity when it is located outside Canada. The proposed amendment would ensure that, in these circumstances, the local agent in Canada would be subject to all of the obligations under the PCMLTFA.

Compliance Issues

6.12 Compliance Regime

Reference: PCMLTFA, Part 3

Amendment

Include an explicit requirement in the PCMLTFA for reporting entities to implement a compliance regime.

Explanation

The requirement for reporting entities to establish a compliance regime is linked to their obligations under Part 1 of the Act. This requirement is prescribed in the regulations, but not in the Act. The proposed amendment would add clarity and certainty by adding an explicit corresponding requirement under the Act.

6.13 Providing Documents to Compliance Officers

Reference: PCMLTFA, section 5

Amendment

Require that documents requested by a FINTRAC compliance officer be produced at a site determined by FINTRAC.

Explanation

The amendment would allow FINTRAC to conduct examinations in its own offices and avoid having to request a search warrant for reporting entities that operate in dwelling houses that deny FINTRAC access to their premises.

6.14 Compliance Questionnaires

Reference: PCMLTFA, section 62

Amendment

Require that reporting entities complete and return compliance questionnaires sent by FINTRAC.

Explanation

Currently, reporting entities are not compelled to complete compliance questionnaires. The amendment would allow FINTRAC to require that these questionnaires be completed and returned for risk-assessment purposes.

6.15 Statute of Limitations for Non-Compliance Infractions

Reference: PCMLTFA, Part 5

Amendment

Extend to five years the one-year limit in respect of non-compliance infractions proceeding by summary conviction.

Explanation

Currently, the statute of limitations for non-compliance infractions is one year in the event that the Crown elects to proceed by summary conviction. Extending to five years the statute of limitations for non-compliance infractions proceeding by summary conviction would provide the Crown greater flexibility to determine if it wishes to prosecute a non-compliance infraction.

6.16 Reporting Entities Going Out of Business

Reference: PCMLTFA, Part 3

Amendment

Transfer the obligations under the Act of a company that is no longer in business to its directors.

Explanation

Currently, it is difficult to hold companies that no longer exist accountable for non-compliance violations that the company may have engaged in while in business. The proposed amendment would be to transfer continued responsibility for those violations to the director(s) of the corporation in the event that it ceases to be a legal entity.

6.17 Documents Protected by Solicitor-Client Privilege

Reference: PCMLTFA, sections 62 to 65

Amendment

Amend the compliance provisions that allow FINTRAC to examine documents to bring the PCMLTFA into conformity with the principles set out by the Supreme Court of Canada in its decision in the case of *Lavallee, Rackel & Heintz* in respect of solicitor-client privilege.

Explanation

In a 2002 decision in the case of *Lavallee, Rackel & Heintz*, the Supreme Court of Canada set out principles that should be followed to protect solicitor-client privilege when the police seize documents from law offices under warrants. The proposed amendments would ensure that the compliance provisions under the PCMLTFA allowing FINTRAC to examine documents are consistent with these principles.

Disclosures of Information by FINTRAC

6.18 Seeking of Production Orders by the Canada Revenue Agency

Reference: PCMLTFA, section 60

Amendment

Allow the CRA to apply to the court for a production order to obtain additional information from FINTRAC following a disclosure.

Explanation

Although FINTRAC disclosures are limited to key identifying information, the Act allows law enforcement agencies or CSIS, in relation to a money laundering or terrorist financing investigation, to apply to the courts for a production order to obtain the complete case analysis produced by FINTRAC. The proposed amendment would allow the CRA, when engaged in a tax evasion investigation, to seek a production order in relation to a disclosure received from FINTRAC.

6.19 Disclosures to the Communications Security Establishment

Reference: PCMLTFA, section 55

Amendment

Require FINTRAC to disclose information to the Communications Security Establishment (CSE).

Explanation

The proposed amendment would allow FINTRAC, consistent with the Centre's existing mandate, to disclose designated information to CSE in support of its foreign intelligence mandate. This information would assist CSE in its foreign intelligence collection, which in turn would support the Government's national security priorities.

6.20 Disclosure of Customs Information

Reference: PCMLTFA, section 55

Amendment

Require FINTRAC to disclose information related to illegal importations to the Canada Border Services Agency (CBSA).

Explanation

The proposed amendment would require FINTRAC to disclose information to the CBSA when, in addition to a suspicion of money laundering or terrorist activity financing, it also determines that the information would be relevant to an offence related to the importation of goods which are prohibited, controlled or regulated under the Customs Act or other statutes.

6.21 Disclosure of Immigration Information

Reference: PCMLTFA, paragraph 55(3)(d)

Amendment

Eliminate the "promotion of international justice and security" as a condition for disclosure to CBSA Immigration.

Explanation

The proposed amendment would simplify the threshold that FINTRAC must meet in order to disclose information to CBSA Immigration. The requirement that the information be relevant to determine the admissibility of a person in Canada or any violation of the Immigration and Refugee Protection Act would remain, but the requirement in respect of the "promotion of international justice and security" would be removed.

6.22 Refusal to Disclose Information

Reference: PCMLTFA, subsection 60.1 (7)

Amendment

Add national security as grounds for refusal by FINTRAC to disclose information in respect of a production order.

Justification

The Act allows FINTRAC to refuse to disclose certain information under a production order even when it meets the legal thresholds for disclosure to law enforcement and other agencies. The proposed amendment would explicitly add national security as grounds for such refusal.

6.23 Providing Feedback to Foreign Financial Intelligence Units

Reference: PCMLTFA, section 56

Amendment

Clarify that FINTRAC is allowed to provide case-specific feedback on disclosures received from foreign FIUs.

Explanation

The current legislation does not contemplate the provision of feedback to foreign FIUs on the quality of information/disclosures provided to FINTRAC pursuant to the information-sharing provisions of the Act. FINTRAC's MOU partners have requested feedback in the context of individual case disclosures to FINTRAC to assist them in their performance evaluation processes. The proposed amendment would clarify that FINTRAC can provide feedback to its MOU partners indicating the usefulness of this information and how it was utilized to support FINTRAC's operations.

Cross-Border Currency Reporting

6.24 Appeal Provisions for Currency Seizures

Reference: PCMLTFA, sections 24, 29 and 30

Amendment

Clarify that the statutory appeal provisions for currency seizures under Part 2 of the Act apply in respect of the determination that the reporting requirement was contravened.

Explanation

Part 2 of the Act allows an appeal of the Minister's decision in respect of seized currency by way of an action in the Federal Court. The proposed amendment would clarify that this appeal provision applies in respect of the determination that the reporting requirement was contravened, but not in respect of the amount of the penalty assessed or the decision to forfeit the currency. The proposed amendment would make the provision consistent with similar provisions under the Customs Act

6.25 Third Party Claims on Seized Currency

Reference: PCMLTFA, section 32

Amendment

Extend the third party claim provisions in respect of currency seized under Part 2 of the Act to entities such as corporations.

Explanation

Section 32 of the Act allows any "person" who has an ownership interest and who has not contravened the Act to apply for an order declaring its interest in seized currency. However, section 2 of the Act defines the word "person" only as an individual. The proposed amendment would clarify that corporations can also make such applications.

6.26 Sharing of Currency Seizure Information

Reference: PCMLTFA, section 36

Amendment

Allow the CBSA to exchange information on the seizure of unreported currency with its counterparts in other countries.

Explanation

Part 2 of the Act allows the CBSA to enter into an agreement with the customs service of another country to exchange information contained in cross-border currency reports. The proposed amendment would also allow the CBSA to exchange seizure and other information in respect of the cross-border currency reporting regime that is relevant to money laundering or terrorist financing activities.

6.27 Sharing of Information Within the Canada Border Services Agency

Reference: PCMLTFA, section 36

Amendment

Allow the CBSA to share cross-border reporting information internally when it would be relevant in the administration of immigration legislation as well as for the collection of certain taxes and duties.

Explanation

The current information protection provisions prevent CBSA officers from using information obtained in the course of administering Part 2 of the Act for other purposes. The proposed amendment would allow CBSA officers to use this information to fulfill its immigration and tax collection role.

6.28 Cancelling of a Seizure

Reference: PCMLTFA, section 18

Amendment

Allow a customs officer to cancel a currency seizure or reduce a penalty in respect of unreported currency.

Explanation

A person from whom unreported currency was seized under Part 2 of the Act must follow the procedures set out in the legislation to request a decision of the Minister when they believe that the seizure is not justified. The proposed amendment would allow, in certain cases, a customs officer to immediately cancel the seizure or reduce the penalty without the need for the owner of the currency to go through the legislative procedures. This change would make the seizure provisions under the PCMLTFA consistent with the provisions under the Customs Act.

6.29 Sharing of Information with the Canada Revenue Agency

Reference: PCMLTFA, section 36

Amendment

Allow the CBSA to share currency seizure information with the CRA to determine the tax implications.

Explanation

Current information protection provisions prevent CBSA customs officers from sharing information obtained in the course of administering Part 2 of the Act, with the exception of FINTRAC and law enforcement. The proposed amendment would allow CBSA

customs officers to share with the CRA information on seized currency or monetary instruments so that the CRA can determine whether there are any tax implications associated with the currency seizure or the related parties.

6.30 Criminal Penalties

Reference: PCMLTFA, section 74

Amendment

Establish criminal penalties for non-reporting under Part 2 of the Act.

Explanation

Currently, a person failing to report the importation or exportation of currency or monetary instruments under Part 2 of the Act is subject to a monetary penalty. The proposed amendment would provide for criminal fines or jail terms in certain circumstances, such as in the case of repeat offenders and when very elaborate methods are used for the concealment of currency to avoid reporting. The amendment would be consistent with similar existing provisions under the Customs Act.

Chapter 7
Technical Amendments

The Government is also proposing a number of technical amendments.

Legislative Amendments

7.1 Section 2

Amendment

Amend the definition of "terrorist activity financing offence" to expressly include the offence of a "conspiracy or an attempt to commit, being an accessory after the fact in relation to, or any counseling in relation to, a terrorist activity financing offence".

Explanation

The proposed amendment would ensure consistency with the Criminal Code.

7.2 Paragraph 54(d)

Amendment

Replace the references to subsections 55(4) and (5) with subsections 55.1(1) and 56.1(1) respectively.

Explanation

Subsections 55(4) and (5) were replaced with subsections 55.1(1) and 56.1(1) respectively.

7.3 Subsection 59(1)

Amendment

Add a reference to production orders under section 60.

Explanation

The current provision refers only to production orders under section 60.1 of the Act (production orders from CSIS). The proposed amendment would add a reference to production orders from the Attorney General of Canada under section 60.

7.4 Section 65

Amendment

Amend the French wording to make it consistent with the English.

Explanation

The amendment would ensure the consistency of the section in both languages.

Regulatory Amendments (PCMLTF Regulations)

7.5 Subsection 63(4)

Amendment

Replace the reference to subsection 58(3) with 58(2).

Explanation

Subsection 58(2) includes the relevant provisions applicable to corporations while subsection 58(3) deals with entities other than corporations.