Canada’s Anti-Money Laundering & Anti-Terrorist Financing Requirements

A GUIDE FOR CHARTERED ACCOUNTANTS
Canada’s Anti-Money Laundering & Anti-Terrorist Financing Requirements
A GUIDE FOR CHARTERED ACCOUNTANTS

This publication was originally published by The Canadian Institute of Chartered Accountants in 2008. It has been reissued by Chartered Professional Accountants of Canada.
NOTICE TO READER

This Guide has been prepared to assist CAs in understanding Canada’s Anti-Money Laundering and Anti-Terrorist Financing Legislation. It has not been adopted, endorsed, approved, disapproved or otherwise acted upon by a Board, the governing body or membership of the CICA or any provincial Institute/Ordre.

The Guide is not intended to provide legal advice. Neither the CICA nor the individuals involved in its preparation can accept any responsibility for reliance on the contents of this Guide.

Readers should consult the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, as well as the supporting *Regulations*. For additional guidance, readers should also consult the *FINTRAC office consolidation of the Act*, the *FINTRAC office consolidation of the regulations*, and the *FINTRAC Guidelines*.

This Guide is available in PDF format on the CICA website (www.cica.ca).
FOREWORD

The Proceeds of Crime (Money Laundering) Act (PCMLA) was enacted on June 29, 2000. In December 2001, the Anti-Terrorism Act was enacted and included certain amendments to the PCMLA which became the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). The PCMLTFA, together with the Regulations, make it mandatory for various individuals and entities, including chartered accountants (CAs) and accounting firms, to implement a compliance program in accordance with the Guidelines established by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). The objective is to assist in the detection and deterrence of money laundering and terrorist financing, and to facilitate the investigation of money laundering offences and terrorist financing activities.

Chartered accountants are not on the “front line” in the war against money laundering and terrorist financing! But, engaging in certain activities as financial intermediaries on behalf of clients will trigger legal obligations. There are significant penalties for non-compliance, including incarceration and fines of up to $2 million.

The objective of this Guide is:

- to assist CAs in understanding the requirements of the PCMLTFA and Regulations; and
- to outline the responsibilities of CAs flowing from those requirements.

The CICA expresses its appreciation to the members of the Anti-Money Laundering Advisory Committee for the time and effort spent on this initiative and to the following individuals for their comments and advice during the preparation of the original (June 2002) version of the Guide: George Begic, LLB; Barry Elkin, CA; Joanna L. Maund, FCA; Ian A. Murray, FCA; Ronald T. Smith, CA•IFA; and Eric R. Turner, CA. The work undertaken by J. Paul-Émile Roy, CA, Principal, Research Studies, in preparing and updating the Guide is also appreciated.

Toronto, June 2008

CICA Research Studies
CICA ANTI-MONEY LAUNDERING ADVISORY COMMITTEE

Chair
H.M. Wasserman, CA●CIRP, CFE, CFI
Wasserman Associates Inc.
Toronto, Ontario

Members
E.A. Cowie, LL.B
Institute of Chartered Accountants of Ontario
Toronto, Ontario

I.M. Enhagen, CA
Institute of Chartered Accountants of Ontario
Toronto, Ontario

R.T. Hollingshead, CA
PricewaterhouseCoopers LLP
Toronto, Ontario

J.M. Lowry, CA
Investors Choice Financial Management Ltd.
Mississauga, Ontario

B. Soave
Soave Strategy Group
Concord, Ontario

CICA
J.P. Roy, CA
Principal, Knowledge Development Group
Canadian Institute of Chartered Accountants
Toronto, Ontario

E.R. Turner, CA
Principal, Standards Group
Canadian Institute of Chartered Accountants
Toronto, Ontario
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>v</td>
</tr>
<tr>
<td><strong>Chapter 1 — ABOUT MONEY LAUNDERING</strong></td>
<td></td>
</tr>
<tr>
<td>What is Money Laundering?</td>
<td>1</td>
</tr>
<tr>
<td>What is Terrorist Financing?</td>
<td>2</td>
</tr>
<tr>
<td>Money Laundering in Canada</td>
<td>2</td>
</tr>
<tr>
<td>A multi-billion dollar problem</td>
<td>3</td>
</tr>
<tr>
<td>Enacting federal legislation</td>
<td>3</td>
</tr>
<tr>
<td>Financial Transactions and Reports Analysis Centre of Canada</td>
<td>5</td>
</tr>
<tr>
<td>Who must report to FINTRAC?</td>
<td>6</td>
</tr>
<tr>
<td>What are the obligations of CAs and CA firms?</td>
<td>8</td>
</tr>
<tr>
<td><strong>Chapter 2 — IMPLEMENTING A COMPLIANCE PROGRAM</strong></td>
<td></td>
</tr>
<tr>
<td>Compliance Requirements</td>
<td>9</td>
</tr>
<tr>
<td>Designing a Compliance Program</td>
<td>10</td>
</tr>
<tr>
<td>Obtaining a commitment from senior management</td>
<td>10</td>
</tr>
<tr>
<td>Appointing a compliance officer</td>
<td>10</td>
</tr>
<tr>
<td>Developing compliance policies and procedures</td>
<td>11</td>
</tr>
<tr>
<td>Applying a risk-based approach</td>
<td>14</td>
</tr>
<tr>
<td>Monitoring the effectiveness of the compliance program</td>
<td>15</td>
</tr>
<tr>
<td>Providing ongoing training for employees and agents</td>
<td>16</td>
</tr>
<tr>
<td>How will FINTRAC ensure Compliance?</td>
<td>17</td>
</tr>
<tr>
<td><strong>Chapter 3 — SUSPICIOUS TRANSACTIONS</strong></td>
<td></td>
</tr>
<tr>
<td>Reporting Suspicious Transactions</td>
<td>19</td>
</tr>
<tr>
<td>Identifying Suspicious Transactions</td>
<td>20</td>
</tr>
<tr>
<td>Preparing and Transmitting Reports</td>
<td>24</td>
</tr>
<tr>
<td>Reporting Transactions Related to Terrorist Property</td>
<td>25</td>
</tr>
<tr>
<td>Keeping Records of Suspicious Transactions</td>
<td>25</td>
</tr>
<tr>
<td>Legal Liability and Client Communications</td>
<td>26</td>
</tr>
</tbody>
</table>
Chapter 4 — PRESCRIBED TRANSACTIONS

Reporting Prescribed Transactions ................................................................. 27
Preparing and Transmitting Reports ............................................................. 27
Keeping Records of Large Cash Transactions ............................................. 30
  Large cash transaction record ................................................................. 30
  Identity of person or entity involved in a large cash transaction .............. 31
  Acting on behalf of a third party ............................................................. 32
  Third party disclosure statement ............................................................ 32
  Receipt of funds record .................................................................. 32
Legal Liability and Client Communications .................................................. 33

Chapter 5 — CROSS-BORDER CURRENCY AND MONETARY INSTRUMENTS

Cross-Border Currency and Monetary Instrument Reporting (CCMIR) ........... 35
Opening Mail and Disclosing Information ................................................... 36
Legal Liability and Client Communications .................................................. 36

Chapter 6 — RULES OF PROFESSIONAL CONDUCT

Complying with the Rules of Professional Conduct .................................... 37
Duty of Confidence .............................................................................. 37
Unlawful Activity .............................................................................. 38

Chapter 7 — IMPLICATIONS FOR PRACTITIONERS INVOLVED IN AUDIT, REVIEW AND COMPILATION ENGAGEMENTS

Audit Engagement Considerations ............................................................ 41
Review Engagement Considerations ......................................................... 42
Compilation Engagement Considerations .................................................. 42

Appendices

A  Money Laundering Methods and Examples ........................................... 43
B  International Money Laundering Developments ..................................... 47
C  Indicators of Suspicious Transactions ................................................... 55
D  Readiness Assessment Checklist for CAs and CA Firms ........................ 61

Glossary ............................................................................................... 63
Selected Bibliography ............................................................................ 67
EXECUTIVE SUMMARY

The objective of this Guide is to assist CAs in understanding Canada’s anti-money laundering requirements and to outline the responsibilities flowing from those requirements.

About Money Laundering
In Canada, money laundering is an illegal activity that covers any act or attempted act to disguise the source of money or assets derived from criminal activity. It involves a process whereby “dirty money” is transformed into “clean money,” the criminal origin of which is difficult to trace. Dirty money is generated by crimes such as drug trafficking, murder, robbery, bribery, fraudulent manipulation of stock exchange transactions, possessing, issuing or circulating counterfeit money, theft, extortion, forgery and fraud. With new dirty money constantly being introduced into the financial system, the money laundering process is continuous.

Canada’s national initiative to combat money laundering was launched in 1999. Following the events of September 11, 2001, the mandate was extended to include the fight against terrorist financing activities. The initiative is now referred to as the Anti-Money Laundering and Anti-Terrorist Financing Regime. One of the key elements of this Regime is the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). The PCMLTFA facilitates investigations and prosecutions of money laundering and terrorist activity financing offences.

Since the PCMLTFA and related regulations first came into force, the domestic and international environment has changed. First, the international standards of the Financial Action Task Force (FATF) were revised in 2003 to keep up with new money laundering and terrorist financing trends and techniques. As a member of the FATF, Canada is expected to comply with the revised recommendations to ensure the security and integrity of Canada’s financial system and economy in addition to sending a signal to the international community about Canada’s commitment to fight financial crimes.

Second, several of the partners to the Regime, such as the Royal Canadian Mounted Police, the Canada Border Services Agency, the Canada Revenue Agency and the Financial Transactions and Reports Analysis Centre of Canada proposed amendments to help them better fulfill their mandates. Third, a few financial institutions and intermediaries requested changes to the Regime to allow them to concentrate their efforts in areas where the risk of money laundering or terrorist financing is higher. In response to these developments, Canada strengthened the PCMLTFA in December 2006 and amended the regulations during 2007 and early 2008.

The PCMLTFA creates a mandatory reporting system and establishes an independent anti-money laundering agency called the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). FINTRAC’s mandate is to collect, analyze, assess and, where appropriate, disclose information relevant to the investigation and prosecution of money laundering and terrorist financing offences. A series of Regulations and FINTRAC Guidelines support the new legislation.
Application to CAs and CA Firms

Exhibit 1 highlights key sections of the PCMLTFA. Part 1 of the PCMLTFA deals with record keeping and reporting of suspicious transactions and prescribed financial transactions. It applies to persons and entities serving as financial intermediaries on behalf of a client. CAs and CA firms are financial intermediaries when they engage in, or give instructions with regard to any of the following activities on behalf of any person or entity:

• receiving or paying funds,
• purchasing or selling securities, real property or business assets or entities, or
• transferring funds or securities by any means.

It is important to note, however, that Part 1 of the PCMLTFA does not apply in respect of:

• audit, review or compilation engagements carried out in accordance with the Recommendations set out in the CICA Handbook.
• CAs who are employees or agents of a person or entity covered by the PCMLTFA;
• CAs who are employees or agents of a person or entity (third party) not covered by the PCMLTFA.

Part 2 of the PCMLTFA deals with the reporting of cross-border transfers of currency or monetary instruments at or above a specified threshold. Unlike Part 1, which applies only to specified persons and entities, Part 2 applies to all persons and entities including CAs and CA firms, whether or not they serve as financial intermediaries on behalf of their clients.

Implementing a Compliance Program

The Part 1 Regulations require CAs and CA firms that serve as financial intermediaries to implement a compliance program which includes, as far as practicable:

• Obtaining a commitment from senior management;
• Appointing a compliance officer;
• Developing compliance policies and procedures;
• Applying a risk-based approach to money laundering and terrorist financing;
• Monitoring the effectiveness of the compliance system;
• Providing ongoing training for employees and agents.

The compliance program covers the recording and reporting of suspicious transactions and prescribed financial transactions, as well as reporting cross-border transfers of currency or monetary instruments at or above a specified threshold.

FINTRAC is responsible for ensuring compliance with the PCMLTFA. To this end, it is given the authority to examine a person or entity’s compliance program and records. In addition to periodic feedback on the adequacy, completeness and timeliness of the information reported, financial intermediaries may be subject to compliance search and seizure. FINTRAC has the power to enter the premises of a financial intermediary at any reasonable time, without a search warrant, to determine whether they are complying with their obligations to report and record transactions. There are significant penalties for those who fail to comply with these obligations. For example, a conviction for failing to report a suspicious transaction or to make a terrorist property report could result in up to five years imprisonment and/or a fine of $2,000,000.
Exhibit 1

Proceeds of Crime (Money Laundering) and Terrorist Financing Act
Mandatory Reporting Requirements

PART 1

Section 6 — Record keeping
Every person or entity referred to in section 5 shall keep and retain prescribed records in accordance with the regulations. 1

Section 7 — Transactions if reasonable grounds to suspect
In addition to the requirements of subsection 9(1), every person or entity shall report to the Centre, in the prescribed form and manner, every financial transaction that occurs in the course of their activities and in respect of which there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering offence or a terrorist activity financing offence.

7.1 (1) In addition to the requirements of section 7 and subsection 9(1), every person or entity that is required to make a disclosure under section 83.1 of the Criminal Code shall also make a report on it to the Centre, in the prescribed form and manner.

Section 8 — No disclosure of reports
No person or entity shall disclose that they have made a report under section 7, or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun.

Section 9 — Prescribed financial transactions
(1) Subject to section 10.1, every person or entity referred to in section 5 shall report to the Centre, in the prescribed form and manner, every prescribed financial transaction that occurs in the course of their activities.

Limitation
(2) Subsection (1) does not apply to prescribed persons or entities, or prescribed classes of persons or entities, in respect of prescribed transactions, classes of transactions, clients or classes of clients, if the prescribed conditions are met.

List of persons
(3) Every person or entity referred to in section 5 shall establish and maintain a list, in the prescribed form and manner, of their clients in respect of whom a report would have been required under subsection (1) were it not for subsection (2). However, a person or an entity may choose to report a client’s transactions under subsection (1) instead of maintaining the list in respect of that client.

PART 2

Section 12(1) — Currency and monetary instruments
Every person or entity referred to in subsection (3) shall report to an officer, in accordance with the regulations, the importation or exportation of currency or monetary instruments of a value equal to or greater than the prescribed amount.

1 PCMLTFA Section 73(1) states “The Governor in Council may, on the recommendation of the Minister, make any regulations that the Governor in Council considers necessary for carrying out the purposes and provisions of this Act…”
Suspicous Transactions
CAs and CA firms that serve as financial intermediaries must report transactions to FINTRAC when there are reasonable grounds to suspect that the transactions are related to the commission of a money laundering offence or a terrorist activity financing offence. What is a suspicious transaction? There is no ready definition, so professional judgment comes into play.

Guidance on identifying and reporting suspicious transactions is provided in FINTRAC Guidelines. The Guidelines list common indicators that might be useful in assessing whether a transaction is suspicious and should be reported. They also provide several lists of industry-specific indicators compiled in consultation with reporting entities, law enforcement agencies and international financial intelligence organizations.

The Regulations require that records be kept for suspicious transactions. Keeping such records helps to demonstrate compliance, if the need arises. Also, it is important to note that suspicious transactions, whether they are attempted or completed, must be reported.

Prescribed Transactions
CAs and CA firms that serve as financial intermediaries must keep a large cash transaction record, unless the cash is received from a financial entity or a public body. They must also:
- ascertain the identity of the person involved in the transaction;
- take reasonable measures to determine whether the individual who gives the cash is acting on behalf of a third party;
- keep a record when the individual is acting on behalf of a third party, or if there are reasonable grounds to conclude this is the case.

CAs and CA firms that serve as financial intermediaries are required to report the following financial transactions:
- large cash transactions involving amounts of $10,000 or more;
- sending or receiving of international electronic funds transfers of $10,000 or more;
- foreign exchange transactions at a rate that exceeds the posted rate, and the payment by an individual of transaction fees that exceed the posted fees.

Instructions for preparing large cash transaction reports and electronic funds transfer reports are available in FINTRAC Guidelines.

Recent amendments to the Regulations state that a receipt of funds record must be prepared for any amount of $3,000 or more, whether or not it is received in cash. The required information and supporting documentation for these records are specified in FINTRAC Guidelines.

Cross-border Currency and Monetary Instrument Reporting (CCMIR)
Part 2 of the PCMLTFA requires that certain cross-border transfers of currency or monetary instruments be reported to the Canada Border Services Agency (CBSA). The form and manner of reporting are explained in the “Cross-border Currency and Monetary Instruments Reporting Regulations.” Persons or entities sending or “exporting” cash or monetary instruments of $10,000 or more across Canada’s borders must complete a CCMIR report. In turn, the CBSA must send copies of the CCMIR reports to FINTRAC.
Rules of Professional Conduct
Of particular relevance to the issue of money laundering are the Rules of Professional Conduct with respect to the duty of confidence and association with unlawful activities. In this regard, a CA or CA firm serving as a financial intermediary should develop a communications strategy to disclose, in writing, the reporting obligations and other requirements under the PCMLTFA. Furthermore, they must not knowingly lend themselves or their services to any unlawful activity. They must be mindful of the possibility of money laundering and knowingly or unknowingly becoming a party to the offence by failing to take appropriate action.

Implications for Practitioners involved in Audit, Review and Compilation Engagements
As previously noted, the PCMLTFA does not apply to audit, review or compilation engagements carried out in accordance with the recommendations set out in the CICA Handbook – Assurance. Although they have no statutory reporting responsibility with respect to money laundering and terrorist financing activities, practitioners involved in such engagements may encounter circumstances where the proceeds of crime are, or may be, laundered. In such cases, they should be aware of the appropriate action to take to avoid potentially serious consequences and obtain legal advice, if necessary.

Keeping Up with New Developments
FINTRAC provides a significant amount of guidance in the form of Guidelines and Interpretation Notices that can assist reporting entities in keeping up with new developments that may affect them. FINTRAC also conducts ongoing outreach programs for all reporting entities. Chartered accountants and accounting firms that are subject to the PCMLTFA can keep up to date by regularly visiting the FINTRAC website and the CICA’s Online Anti-Money Laundering Resource Centre.
x Canada’s Anti-Money Laundering & Anti-Terrorist Financing Requirements
– A Guide for Chartered Accountants
Chapter 1

ABOUT MONEY LAUNDERING

There are as many methods to launder money as the imagination allows, and the money laundering schemes being used are becoming increasingly sophisticated and complex as technology advances.

WHAT IS MONEY LAUNDERING?
Money laundering is “any act or attempted act to disguise the source of money or assets derived from criminal activity.” Essentially, money laundering is the process whereby “dirty money” — produced through criminal activity — is transformed into “clean money,” the criminal origin of which is difficult to trace.

The money laundering process is continuous, with new dirty money constantly being introduced into the financial system. There are three recognized stages in the money laundering process.

- **Placement** involves placing the proceeds of crime in the financial system.
- **Layering** involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds. This stage may involve transactions such as the buying and selling of stocks, commodities or property.
- **Integration** involves placing the laundered proceeds back into the economy to create the perception of legitimacy.

Appendix A explains some common money laundering methods and provides a variety of illustrative case examples. Under Canadian law, a money laundering offence involves concealing or converting property or the proceeds of property (for example, money), knowing or believing that these were derived from the commission of an offence referred to in Section 462.31 of the **Criminal Code**.

---

2 Refer to [FINTRAC Guideline 1: Backgrounder](#) for a general discussion of money laundering processes.

3 [CAmagazine (October 2001)](#) addresses money laundering and what the legislation means for CAs. It provides considerable insight on money laundering issues.

4 **Criminal Code** Part XII.2 “Proceeds of Crime, Section 462.31 (1) states “Every one commits an offence who uses, transfers the possession of, sends or delivers to any person or place, transports, transmits, alters, disposes of or otherwise deals with, in any manner and by any means, any property or any proceeds of any property with intent to conceal or convert that property or those proceeds, knowing or believing that all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of (a) the commission in Canada of a designated offence; or (b) an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence. Subsection 462.31 (2) states “Every one who commits an offence under subsection (1) (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or (b) is guilty of an offence punishable on summary conviction.”
In Canada, money laundering is an illegal activity. Money laundering offences derive from illegal acts, such as drug trafficking, murder, robbery, bribery, fraudulent manipulation of stock exchange transactions, possessing, issuing or circulating counterfeit money, theft, extortion, forgery and fraud. A money laundering offence may also extend to property or proceeds derived from illegal activities that took place outside Canada.

WHAT IS TERRORIST FINANCING?
Terrorist financing provides funds for terrorist activity. The main objective of terrorist activity is to intimidate a population or compel a government to do something by intentionally killing, seriously harming or endangering a person, by causing substantial property damage that is likely to seriously harm people, or by seriously interfering with or disrupting essential services, facilities or systems.

There are two primary sources of financing for terrorist activities. The first source of financing is getting financial support from countries, organizations or individuals. In this regard, terrorism could be sponsored by a country or government, although this is believed to have declined in recent years. State support may be replaced by support from other sources, such as individuals with sufficient financial means.

The second source of financing involves revenue-generating activities which may include criminal acts. Terrorist groups may use kidnapping, extortion, smuggling, fraud, theft, robbery and narcotics trafficking to generate funds. Like criminal organizations, they have to find ways to launder these illicit funds to be able to use them without drawing the attention of the authorities. For this reason, transactions related to terrorist financing may look a lot like those related to money laundering. Therefore, strong, comprehensive anti-money laundering regimes are key to also tracking terrorist financing activities.

MONEY LAUNDERING IN CANADA
In Canada, money laundering is an integral element of organized criminal activity, and is the proven method by which organized crime groups seek to transform the proceeds of drug trafficking, contraband goods and people smuggling, extortion and other activities into apparently legitimately earned funds. Laundered proceeds of crime provide seemingly legitimate financial support to drug dealers, terrorist organizations, arms dealers and other criminals to amass wealth and operate and expand their criminal empires. It is clear that the problem is enormous. It increases rapidly when one considers that the money laundering statutes apply to tax evasion, trade fraud and bank, medical and insurance fraud.

---

5 The US, in 1986, was the first country in the world to criminalize money laundering, but only as it related to the illegal drug trade. In 1990, Canada passed legislation that identified money laundering as a criminal offence.
A multi-billion dollar problem
Investigations have revealed that those involved in money laundering manipulate financial systems in Canada and abroad to foster a wide range of illicit activities. The economic and political influence of criminal organizations can potentially weaken the social fabric, collective ethical standards and, ultimately, the democratic institutions of society. Money laundering activities also have the potential to distort economic data and to cause economic growth to suffer.

In fact, studies by the International Monetary Fund on the relationship between gross domestic product growth and money laundering in industrial countries have found evidence that significant reductions in annual gross domestic product growth rates were associated with increases in money laundering activities. The studies show that the aggregate amount of money being laundered in the world could be somewhere between two and five percent of world gross domestic product, or between approximately C$900 billion and C$2.25 trillion.

The sheer magnitude of money laundering activities demonstrates the importance of implementing strong anti-money laundering regimes in countries throughout the world. The increasingly international character of business and the transnational nature of money laundering activities have resulted in stepped up international efforts and cooperation in the fight against money laundering.

International anti-money laundering standards have been established by the Financial Action Task Force (FATF), of which Canada is a member. Since money laundering is global in scope, it is important that Canada enhance its contribution to international efforts to deter and detect money laundering.

Enacting federal legislation
To combat money laundering, the Canadian federal government enacted the Proceeds of Crime (Money Laundering) Act, which received Royal Assent on June 29, 2000. To help fight terrorism, it enacted the Anti-Terrorism Act (Bill C-36). The Anti-Terrorism Act (ATA), which came into force on December 24, 2001, amends the Criminal Code, the Canadian Human Rights Act, and the Proceeds of Crime (Money Laundering) Act, which becomes the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

---

6 Studies by the Solicitor General of Canada have estimated that billions in criminal proceeds are laundered in and through Canada every year. The experience of other countries can provide considerable insight into law enforcement efforts. Appendix B of this Guide provides an overview of international developments.

7 It is estimated that over 80% of all money laundering schemes have an international dimension. For examples, refer to “Money Laundering: A Banker’s Guide to Avoiding Problems” issued in December 2002 by the Office of the Comptroller of the Currency (OCC), a bureau of the US Department of the Treasury.

8 The FATF completed an assessment of the implementation of anti-money laundering and counter-terrorist financing standards in Canada in February 2008 (see Mutual Evaluation of Canada).

9 The official title is “An Act to facilitate combating the laundering of proceeds of crime and combating the financing of terrorist activities, to establish the Financial Transactions and Reports Analysis Centre of Canada and to amend and repeal certain Acts in consequence.”

10 The Anti-Terrorism Act received Royal Assent on December 18, 2001. The official title is “An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism.”
The ATA includes significant additions to the Criminal Code to include offences relating to terrorist activities and the financing of terrorism. These changes make it a crime to do any of the following:

- knowingly collect or provide funds, either directly or indirectly, to carry out terrorist activities;
- knowingly participate in, contribute to or facilitate the activities of a terrorist group;
- instruct anyone to carry out a terrorist activity on behalf of a terrorist group; or
- knowingly harbour or conceal a terrorist.

The ATA is central to the Government of Canada’s Anti-Terrorism Plan which has four objectives:

- stop terrorists from getting into Canada and protect Canadians from terrorist acts;
- bring forward tools to identify, prosecute, convict and punish terrorists;
- prevent the Canada-US border from being held hostage by terrorists and impacting upon the Canadian economy; and
- work with the international community to bring terrorists to justice and address the root causes of such hatred.

The ATA expands Canada’s anti-money laundering legislation to include terrorist financing in its objectives. The revised objectives of the PCMLTFA are:

- to implement specific measures to detect and deter money laundering and the financing of terrorist activities, and to facilitate the investigation and prosecution of money laundering offences and terrorist activity financing offences, including:
  - establishing record keeping and client identification requirements for financial services providers and other persons or entities that engage in businesses, professions or activities that are susceptible to being used for money laundering or the financing of terrorist activities,
  - requiring the reporting of suspicious financial transactions and of cross-border movements of currency and monetary instruments, and
  - establishing an agency that is responsible for dealing with reported and other information;
- to respond to the threat posed by organized crime by providing law enforcement officials with the information they need to deprive criminals of the proceeds of their criminal activities, while ensuring that appropriate safeguards are put in place to protect the privacy of persons with respect to personal information about themselves; and
- to assist in fulfilling Canada’s international commitments to participate in the fight against transnational crime, particularly money laundering, and the fight against terrorist activity.

---

11 The objectives are set out in Section 3 of the PCMLTFA.
12 The PCMLTFA establishes the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as the independent federal government agency that will operate at arm’s length from law enforcement agencies.
FINANCIAL TRANSACTIONS AND REPORTS ANALYSIS CENTRE OF CANADA

The *PCMLTFA* creates a mandatory reporting system for suspicious and prescribed transactions and the cross-border movement of large amounts of currency and monetary instruments.\(^\text{13}\) It establishes an independent anti-money laundering agency called the [Financial Transactions and Reports Analysis Centre of Canada](#) (FINTRAC).\(^\text{14}\)

FINTRAC’s mandate is to collect, analyze, assess and, where appropriate, disclose information relevant to the investigation and prosecution of money laundering and terrorist financing offences. FINTRAC is also responsible for conducting research and for undertaking educational measures to inform the public, those who are required to report suspicious transactions and the law enforcement community about the nature and extent of money laundering and terrorist financing activities, and effective detection, prevention and deterrence measures. A series of [Regulations](#) and FINTRAC [Guidelines](#) support the filing of suspicious transaction reports and other reporting obligations under the legislation.\(^\text{15}\)

FINTRAC receives and analyzes reports from financial service providers and those engaged in businesses, professions or activities that are susceptible to being used for money laundering. When it determines that there are reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence, it discloses only designated information to the appropriate police authorities. To obtain further information from FINTRAC, police must first get a court order.

When FINTRAC has made this determination, it may also, under specified circumstances, disclose designated information to the following agencies and departments:

- **Canada Revenue Agency** (CRA), when FINTRAC also determines that the information is relevant to a tax evasion offence;
- **Canadian Security Intelligence Service** (CSIS), when FINTRAC also determines that the information is relevant to threats to the security of Canada; and
- **Citizenship and Immigration Canada**, when FINTRAC also determines that the information would promote the objective set out in paragraph 3(1)(i) of the *Immigration and Refugee Protection Act* — to promote international justice and security by fostering respect for human rights and by denying access to Canadian territory to persons who are criminals or security risks.

---

\(^\text{13}\) In December 1999, the federal government released a Consultation Paper on the Regulations to the *PCMLTFA* to industry and other key stakeholders for comment, including the Canadian Institute of Chartered Accountants.

\(^\text{14}\) FINTRAC was established on July 5, 2000.

\(^\text{15}\) More information on the *PCMLTFA*, money laundering and FINTRAC is available at the FINTRAC website ([www.fintrac.gc.ca](http://www.fintrac.gc.ca)), by e-mail ([guidelines-lignesdirectrices@fintrac-canafe.gc.ca](mailto:guidelines-lignesdirectrices@fintrac-canafe.gc.ca)), or by phone toll-free (1-866-346-8722).
The FINTRAC Guidelines state that individual privacy will be respected and confidential information will be protected. In this regard, Part 3 of the PCMLTFA (Sections 55 to 61) addresses the Disclosure and Use of Information. It provides various safeguards including the following:

- the independence of FINTRAC from law enforcement and other agencies entitled to receive reported information;
- significant criminal penalties for any unauthorized use or disclosure by FINTRAC of the personal information under its control (up to five years imprisonment and/or a fine of $500,000);
- that limited “designated information” may only be disclosed to law enforcement authorities when there are reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;
- the requirement for police to get a court order to obtain more than limited “designated information” from FINTRAC; and
- the application of the federal Privacy Act to FINTRAC.

Who must report to FINTRAC?
Although anyone, including law enforcement agencies, can voluntarily report information about suspicions of money laundering, the following persons and entities are subject to Part 1 of the PCMLTFA:¹⁶

- financial entities (such as banks, credit unions, caisses populaires, trust and loan companies and agents of the Crown that accept deposit liabilities);
- life insurance companies, brokers and agents;
- securities dealers, including portfolio managers and investment counsellors;
- persons engaged in the business of foreign exchange dealing;
- money services businesses (including Canada Post for money orders);
- real estate brokers and sales representatives (when carrying out certain activities on behalf of their clients);
- casinos;
- **accountants and accounting firms (when carrying out certain activities on behalf of their clients);** and
- individuals, whether a Canadian citizen or not, and any entity who is importing or exporting currency or monetary instruments of $10,000 or more.¹⁷

---

¹⁶ Refer to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, Section 5.
¹⁷ According to the Regulations published in 2008, lawyers, dealers in precious metals and stones, and real estate developers will also become reporting entities.
According to the Part 1 Regulations, the *PCMLTFA* applies to “accountants” and “accounting firms.”\(^{18}\) An “accountant” is defined as a chartered accountant, certified general accountant or a certified management accountant. An “accounting firm” is defined as an entity that is engaged in the business of providing accounting services to the public and has at least one partner, employee or administrator that is an accountant.

**Financial intermediaries**

To meet their obligations under Part 1 of the *PCMLTFA*, CAs and CA firms that serve as financial intermediaries on behalf of their clients are required to report to FINTRAC. CAs and CA firms are financial intermediaries when they:\(^{19}\)

(a) engage in any of the following activities on behalf of any person or entity, namely,

- receiving or paying funds,\(^ {20}\)
- purchasing or selling securities, real properties or business assets or entities, or
- transferring funds or securities by any means;

(b) give instructions on behalf of any person or entity in respect of any activity referred to in paragraph (a).\(^ {21}\)

CAs and CA firms are subject to the *PCMLTFA* requirements whether or not they receive professional fees for these activities. That means the requirements apply even if the activities are carried out on a volunteer basis. On the other hand, the legal obligations do not apply to:

- the professional fees themselves;
- audit, review or compilation engagements carried out according to the recommendations in the Canadian Institute of Chartered Accountants (CICA) Handbook;\(^ {22}\)
- advice offered to a client (because advice is different from giving instructions).\(^ {23}\)

---

\(^{18}\) The Part 1 Regulations state, in Section 34 (1), that “every accountant and every accounting firm is subject to Part 1 of the Act” when they serve as financial intermediaries.

\(^{19}\) Identical wording is used in Part 1 Regulations, Section 34 (1) and Suspicious Transactions Reporting Regulations, Section 6(1).

\(^{20}\) “Funds” means cash, currency or securities or negotiable instruments or other financial instruments, in any form, that indicate a person’s or an entity’s title or interest in them.

\(^{21}\) As noted in *FINTRAC Guideline 6: Record Keeping and Client Identification*, it is FINTRAC’s position that “giving advice to a client is not considered as providing instructions.”

\(^{22}\) Identical wording is used in Part 1 Regulations, Section 34 (3) and Suspicious Transactions Reporting Regulations, Section 6(3).

\(^{23}\) According to *FINTRAC Interpretation Notice No. 2* (October 3, 2005) “Giving instructions means that the accountant is actually directing the movement of funds. By contrast, providing advice to their client is not considered to be giving instructions.”
What are the obligations of CAs and CA firms?
The PCMLTFA establishes specific measures to detect, prevent and deter money laundering and terrorist financing activities, and to facilitate the investigation and prosecution of money laundering and terrorist activity financing offences. These measures require financial intermediaries to prepare and file reports, and keep records on certain types of financial transactions.

The Part 1 Regulations call for CAs and CA firms that serve as financial intermediaries to implement a compliance program, report and record suspicious transactions and terrorist property, and report and record prescribed financial transactions. The Part 2 Regulations require every cross-border transfer of currency or monetary instruments of $10,000 or more to be reported to the Canada Border Services Agency in accordance with Section 12 of the PCMLTFA.

Guidance with respect to those obligations is provided in chapters 2 to 5 of this Guide. CAs and CA firms also have a professional responsibility to uphold the Rules of Professional Conduct and to follow generally accepted auditing standards (GAAS) with respect to illegal acts. Guidance on these matters is provided in chapters 6 and 7 of this Guide.
Chapter 2

IMPLEMENTING A COMPLIANCE PROGRAM

The Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations require financial intermediaries to assist FINTRAC by implementing a regime for complying with the Act and supporting Regulations.

COMPLIANCE REQUIREMENTS

As noted in Chapter 1, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) creates a mandatory reporting system for suspicious transactions, prescribed transactions and the cross-border movement of large amounts of currency and monetary instruments. It also establishes an independent anti-money laundering agency called FINTRAC to collect, analyze, assess and, where appropriate, disclose information relevant to the investigation and prosecution of money laundering and terrorist financing offences.

In line with the objectives of the PCMLTFA, the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations establish the following requirement: “For the purposes of paragraph 3(a) of the Act, and to assist the Centre [FINTRAC] in carrying out its mandate under paragraph 40(e) of the Act, every person or entity to which any of the paragraphs 5(a) to (l) of the Act applies shall implement a regime for complying with the Act and any Regulations made under the Act.”

The Regulations call for a compliance regime that includes, as far as practicable: (a) the appointment of a person — who may be the person referred to in subsection (1) — who is to be responsible for the implementation of the regime; (b) the development and application of compliance policies and procedures; (c) a review of those policies and procedures that is conducted as often as necessary to test their effectiveness by an internal or external auditor of the person or entity or, if it does not have such an auditor, by the person or entity itself; and (d) where the person or entity has employees or agents or persons authorized to act on behalf of the person or entity, an on-going compliance training program for those employees, agents or persons.

---

24 Part 1 Regulations, Section 71(1).
25 Part 1 Regulations, Section 71(2).
FINTRAC  *Guideline 4: Implementation of a Compliance Regime* addresses the requirement to implement a program to ensure compliance with the *PCMLTFA*. The Guideline notes that accountants or accounting firms that serve as *financial intermediaries* on behalf of their clients must meet specified reporting, record-keeping and client identification obligations.

Because the nature, size and complexity of operations will vary, a compliance program should be tailored to meet individual needs. The formality of the policies and procedures depends on the needs of the financial intermediary. Generally, the degree of detail, specificity and formality of the regime varies according to the complexity of the issues and transactions the financial intermediary is involved in, as well as the risk of exposure to money laundering.

**DESIGNING A COMPLIANCE PROGRAM**

The following sets out general considerations for developing, implementing and maintaining a money laundering compliance program based on *FINTRAC Guideline 4*. The key elements of an effective program should include, as far as practicable:

- Obtaining a commitment from senior management;
- Appointing a compliance officer;
- Developing compliance policies and procedures;
- Assessing the risks related to money laundering and terrorist financing;
- Monitoring the effectiveness of the compliance program;
- Providing ongoing training for employees and agents.

**Obtaining a commitment from senior management**

A sound compliance program requires clear leadership and a commitment by senior management to prevent, detect and address non-compliance. Accordingly, those assigned responsibility for compliance must be given the decision-making authority to oversee the firm’s practices, including the implementation of appropriate policies and procedures, staff training and compliance testing. Management must also ensure that adequate resources are available for developing a money laundering compliance program and the time frame for implementation should be realistic.

**Appointing a compliance officer**

Designating responsibility for compliance is required by the *PCMLTFA*. The appointed compliance officer should have the authority and the resources necessary to effectively discharge assigned responsibilities. In an accounting firm, the compliance officer should report, on a regular basis, to senior management. The Regulations also allow sole practitioners who are subject to the *PCMLTFA* to appoint themselves as the compliance officer.

---

26 Additional guidance for developing an effective money laundering plan is available from the Office of the Superintendent of Financial Institutions (OSFI) in the guideline titled “*Deterring and Detecting Money Laundering*.”

27 FINTRAC Guideline 4 notes that employees or agents acting on behalf of an accountant or accounting firm are not responsible for implementing a compliance program. The accountant or accounting firm is responsible.
The designation of a responsible individual does not relieve the accounting firm of the obligation to comply with the *PCMLTFA*. Instead, it formally establishes one individual to serve as the intermediary between the firm’s clients and FINTRAC. Assigning responsibility to a compliance officer provides a means for building expertise in effectively managing money laundering issues relating to any of the firm’s operations.

In an accounting firm, the compliance officer should have direct access to senior management and should not be directly involved in the receipt, transfer and/or payment of funds. To ensure consistent and ongoing attention to the compliance regime, the appointed officer may choose to delegate certain duties to other employees. For example, the officer may delegate an individual in a local office or branch to ensure that compliance procedures are properly implemented at that location. That being said, the appointed compliance officer remains responsible for the firm’s overall compliance program.

**Developing compliance policies and procedures**

An effective compliance program should contain written policies and procedures that are approved by a senior officer and kept up to date to ensure proper processing and completion of transactions including:

- a clear definition of roles and responsibilities;
- the supporting processes required;
- citations of the legislative and regulatory requirements (for example, see Exhibit 2.1);
- sample forms and instructions; and
- directions for routing, review and retention of documents.

When assessing what policies and procedures should be implemented, the principles are the same for all financial intermediaries required to have a compliance program. They should consider what specific policies and procedures are needed with respect to the following matters:

- identifying reportable transactions;
- completing and filing reports;
- ascertaining identity.
- record keeping; and
- handling a FINTRAC compliance audit search and seizure.

**Identifying Reportable Transactions**

Policies and procedures should be designed to enable staff to properly identify reportable transactions. As noted in Exhibit 2.1, accountants and accounting firms that serve as financial intermediaries on behalf of their clients must report suspicious transactions and prescribed transactions. Specific guidance on reporting suspicious transactions is provided in Chapter 3 of this Guide. For prescribed transactions, there is a requirement to report all large cash transactions (when an amount of $10,000 or more is received) and the sending or receiving of an international electronic funds transfer of $10,000 or more. Specific guidance on reporting prescribed transactions is provided in Chapter 4 of this Guide. In addition, pertinent guidance with respect to cross border currency and monetary instrument reporting is provided in Chapter 5 of this Guide.
### Exhibit 2.1

**Compliance Requirements**

**for Accountants and Accounting Firms**

<table>
<thead>
<tr>
<th>Reporting</th>
<th>PCMLTFA / Regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious transactions</td>
<td>PCMLTFA Sections 7 &amp; 8</td>
</tr>
<tr>
<td>PCMLTFA Sections 7 &amp; 8</td>
<td>Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations Sections 1(2) definitions, 2, 6, 9, 11, 12(1), 12(2) and Schedule 1</td>
</tr>
<tr>
<td>Terrorist property</td>
<td>PCMLTFA Section 7.1</td>
</tr>
<tr>
<td>PCMLTFA Section 7.1</td>
<td>Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations Sections 1(2) definitions, 2, 6, 10, 11, 12(3) and Schedule 2</td>
</tr>
<tr>
<td>Large cash transactions</td>
<td>PCMLTFA Section 9(1)</td>
</tr>
<tr>
<td>PCMLTFA Section 9(1)</td>
<td>Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations Sections 1(2) definitions, 2, 3, 4, 5(2), 6, 7, 34, 35, 52(1) &amp; (3), 78, Schedule 1</td>
</tr>
<tr>
<td>Cross-border currency and monetary instruments</td>
<td>PCMLTFA Section 12 to Section 39</td>
</tr>
<tr>
<td>PCMLTFA Section 12 to Section 39</td>
<td>Cross-Border Currency and Monetary Instruments Reporting Regulations</td>
</tr>
<tr>
<td>Record Keeping</td>
<td>PCMLTFA Section 6</td>
</tr>
<tr>
<td>Large cash transaction record</td>
<td>Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations Sections 1(2) definitions, 6, 7, 34, 36, 52(2), 68, 69, 70, 78</td>
</tr>
<tr>
<td>Ascertaining Identity</td>
<td>Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations Sections 53, 63, 64(1)(d), 64(2)(b), 64(3), 65, 66, 67, 78</td>
</tr>
<tr>
<td>Third-party Determination</td>
<td>Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations Section 8, 78</td>
</tr>
<tr>
<td>Third-party statement</td>
<td></td>
</tr>
<tr>
<td>(large cash transaction record)</td>
<td></td>
</tr>
</tbody>
</table>
Completing and Filing Reports
Policies and procedures should be designed to ensure that all reportable transactions are properly identified and to ensure that the reports are properly completed and sent to FINTRAC in a timely fashion. For information on how and when to complete and file the reports, persons and entities should consult FINTRAC Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC.

In general, financial intermediaries must send suspicious transaction reports to FINTRAC within 30 days after detecting a fact related to a transaction that constitutes reasonable grounds to suspect that the transaction is related to the commission of a money laundering offence or a terrorist activity financing offence. A report in respect of an electronic funds transfer must be sent to FINTRAC not later than five working days after the day of the transfer. A report in respect of a large cash transaction must be sent to FINTRAC within 30 days after the transaction, but this will be reduced to 15 days after the first year of reporting is completed.

Ascertaining Identity
The Regulations include specific requirements about identifying individuals with whom the persons or entities are conducting a transaction and keeping client identification up to date. Therefore, in the design of compliance policies and procedures, consideration should be given to ensuring compliance with the requirements for ascertaining identity.

Record Keeping
Under the Regulations, persons and entities are required to keep certain records after conducting specified transactions. Therefore, it is essential to have policies and procedures in place to ensure adherence with the record-keeping requirements. Furthermore, the persons and entities should maintain an effective record-keeping system to enable either internal or external auditors or FINTRAC to have access to the records in a timely fashion.

In this regard, records are to be kept such that they can be provided to FINTRAC within 30 days of a request to examine them. The records may be kept in a machine-readable or electronic form, as long as a paper copy can be readily produced. Also, for records that are kept electronically, an electronic signature of the individual who must sign the record must be retained.

Handling a FINTRAC compliance audit search and seizure
In addition to periodic feedback from FINTRAC on the adequacy, completeness and timeliness of the information reported, financial intermediaries may be subject to compliance search and seizure. Under Part 3, Section 62 of the PCMLTFA, a person authorized by FINTRAC has the power to enter the premises of a financial intermediary at any reasonable time, without a search warrant, to determine whether they are complying with their obligations to report and record transactions.
CAs and CA firms must cooperate with FINTRAC and any person authorized by FINTRAC to the extent required by the *PCMLTFA* and the Regulations, taking into consideration their obligations under the *Rules of Professional Conduct*. In the event that FINTRAC representatives enter the premises of a CA or CA firm to conduct a compliance search, proper identification should be obtained and the appointed compliance officer immediately notified. The compliance officer should be responsible for liaising with FINTRAC representatives throughout the course of the compliance search and for keeping records of any searches and seizures made.

In a compliance search, FINTRAC representatives must be given:
- full use and access to the data on any computer or data processing system in the premises;
- the right to examine and reproduce any data in printout or other electronic form; and
- the right to use any copying equipment to make any required copies.

In addition, FINTRAC representatives must be provided with all reasonable assistance to enable them to carry out their responsibilities and any information with respect to the administration of the recording and reporting obligations that they may reasonably require.

**Applying a risk-based approach**

Perhaps the most difficult part of implementing an effective compliance program is building in the risk-based parameters for money laundering and terrorist financing. The risk assessment applies to chartered accountants themselves, as well as to their clients.

FINTRAC elaborates on the risk-based approach in *Guideline 4* (paragraph 6.0):

“In the context of money laundering and terrorist financing, a risk-based approach is a process that encompasses the following:
- the risk assessment of your business activities using certain factors;
- the risk-mitigation to implement controls to handle identified risks;
- keeping client identification and, if required for your sector, beneficial ownership information up to date; and
- the ongoing monitoring of financial transactions that pose higher risks.”

According to FINTRAC, “a risk assessment is an analysis of potential threats and vulnerabilities to money laundering and terrorist financing to which your business is exposed. The complexity of the assessment depends on the size and risk factors of your business.”

To assist with the risk assessment, FINTRAC suggests referring to *Guideline 1: Backgrounder* for additional information on money laundering and terrorist financing and *Guideline 2: Suspicious Transactions* for additional common and industry-specific indicators related to products and services as well as to occupation, business, financial history and past transaction patterns of clients.
FINTRAC states that each reporting entity must assess and document the risk of services related to money laundering and terrorist activity financing in a way that is appropriate to each reporting entity considering:
- clients and business relationships;
- products, services and delivery channels;
- geographic areas where the services are provided or where clients are located;
- other relevant factors related to the business activities.

Regarding risk mitigation, Guideline 4 (paragraph 6.2) explains that: “Risk mitigation is about implementing controls to limit the potential money laundering and terrorist financing risks you have identified while conducting your risk assessment to stay within your risk tolerance level. As part of your compliance program, when your risk assessment determines that risk is high for money laundering or terrorist financing, you have to develop written risk-mitigation strategies (policies and procedures designed to mitigate high risks) and apply them for high risk situations.”

With respect to client identification, Guideline 4 (paragraph 6.3) notes that: “When your risk assessment determines that risk is high for money laundering or terrorist financing, you have to develop and apply policies and procedures to keep client identification information up to date. If you are a financial entity, a securities dealer, a life insurance company, broker or agent, or a money services business, this also applies for keeping beneficial ownership information up to date.”

When it comes to ongoing monitoring, Guideline 4 (paragraph 6.4) says: “You have to take reasonable measures to conduct ongoing monitoring of financial transactions that pose high risks of money laundering and terrorist financing to detect suspicious transactions. Reasonable measures may involve manual or automated processes, or a combination of both depending on your resources and needs. They also depend on the size of your business and the risks to which you are exposed. You do not necessarily have to create or purchase an electronic system. You can use your available resources and business processes and build on these. Your policies and procedures have to determine what kind of monitoring is done for particular high risk situations, including how to detect suspicious transactions. Your policies and procedures should also describe when monitoring is done (its frequency), how it is reviewed, and how it will be consistently applied.”

**Monitoring the effectiveness of the compliance program**

Another component of a comprehensive compliance program is a review, which enables the financial intermediary to monitor its effectiveness. The review should evaluate the need to modify existing policies and procedures (or to implement new ones), as well as the effectiveness of the risk assessment and training. The review should be conducted at least every two years. The appointed compliance officer would play a key role in assessing the need for a review. Several factors could trigger this need, such as changes in legislation, non-compliance issues, and new services or products.
The Regulations require that the internal or external auditors undertake the review of the compliance program.\textsuperscript{28} When the person or entity does not have internal or external auditors, the entity or person could do a “self-review.” When feasible, a self-review should be conducted by an individual who is independent of the reporting, record-keeping and compliance-monitoring functions. This individual could be an employee or an outside consultant.

The objective of the review is to assess the effectiveness of the policies and procedures in ensuring compliance with the \textit{PCMLTFA} and the Regulations. According to FINTRAC Guideline 4, the review should include the following:

\begin{itemize}
    \item interviews with those handling transactions and with their supervisors, to determine their knowledge of the legislative requirements, policies and procedures;
    \item a review of the criteria and process for identifying and reporting suspicious transactions;
    \item a sampling of large cash transactions, followed by a review of the reporting of such transactions;
    \item a sampling of international electronic funds transfers (if those are reportable by the reporting person or entity in question), followed by a review of the reporting of such transactions;
    \item a test of the record-keeping system for compliance with the legislation;
    \item a test of the client identification procedures for compliance with the legislation;
    \item a review of the risk assessment.
\end{itemize}

It is essential that the scope and the results of the review be documented. Deficiencies should be identified and reported to senior management or the board of directors, with a request for a response indicating corrective actions and a timeline for implementing such actions. According to FINTRAC Guideline 4, within 30 days of the review, the following matters must be reported in writing to a senior officer:

\begin{itemize}
    \item the findings of the above review;
    \item any updates that were made to the policies and procedures during the review period;
    \item the status of implementation of the policies and procedures updates.
\end{itemize}

\textbf{Providing ongoing training for employees and agents}

A written, ongoing training program is essential. For all financial intermediaries, the objective of the training is the same. Employees and agents should be aware of the legislative and regulatory requirements, and understand the compliance policies and procedures and their respective responsibilities. The method of training may vary greatly, depending on the size of the financial intermediary, time requirements and the complexity of the subject matter.

Several important elements merit consideration when assessing training needs. Any training should include some background information on money laundering, to provide an understanding of what money laundering is, why criminals choose to launder money, and how the process usually works. The frequency and method of training (for example, formal, on-the-job, external) should be addressed.

\textsuperscript{28} Part I Regulations, Section 71(2).
In general, training should provide employees and agents with:

- an understanding of the reporting, client identification and record-keeping requirements, as well as the penalties for not meeting those requirements;
- an awareness of the policies and procedures for deterring and detecting money laundering and terrorist financing;
- an understanding of assigned responsibilities;
- insight on vulnerabilities to abuse by criminals laundering the proceeds of crime or by terrorists financing their activities;
- examples of how the entity could be used to launder illicit funds or finance terrorist activity;
- the ability to identify suspicious transactions.

All employees, including senior management, who have contact with clients, who see client transaction activity, or who handle cash in any way, should receive training. The training should also include those who have responsibilities under the compliance program, such as information technology staff and others responsible for designing and implementing electronic or manual internal controls, the appointed compliance officer, and internal or external auditors.

New employees and agents should be trained before they begin to deal with clients. Employees and agents should be periodically informed of any changes in anti-money laundering legislation and anti-terrorism legislation, policies and procedures, as well as current developments and changes in money laundering and terrorist activity financing schemes particular to their jobs. Employees and agents who change jobs within the firm should be provided with training, if necessary, to be up to date with the policies, procedures and risks of exposure to money laundering that are associated with their new job.

HOW WILL FINTRAC ENSURE COMPLIANCE?

FINTRAC has a responsibility to ensure compliance with the *PCMLTFA*. To this end, it is given the authority to examine a person or entity’s compliance regime and records. It may also periodically provide feedback to persons and entities to ensure the adequacy, completeness and timeliness of the information reported to FINTRAC.

Part 3 of the *PCMLTFA*, Sections 62 to 65, establishes Compliance Measures that allow FINTRAC to conduct compliance audits of reporting entities. FINTRAC’s compliance program will use risk management strategies to identify persons and entities most in need of improving compliance. FINTRAC will focus its efforts on areas where there is greater risk of non-compliance and in which the failure to comply could have significant impact on the efforts of FINTRAC to detect and deter money laundering and terrorist financing.

Sections 66 and 67 also allow FINTRAC to enter into arrangements with financial sector regulators, provincial governments and self-regulatory organizations for the purpose of exercising its powers. In this regard, FINTRAC will develop and promote a compliance policy that favours a cooperative approach. Where this cooperative approach fails, FINTRAC will consider referring such cases to the appropriate law enforcement agencies.

---

29 *PCMLTFA* Section 40(e).
30 *PCMLTFA* Section 62.
In those situations, Part 5 of the *PCMLTFA*, Sections 74 to 82, deals with Offences and Punishment. Criminal charges and severe penalties could result from a conviction regarding:

- failure to report a suspicious transaction or to make a terrorist property report — up to five years imprisonment and/or a fine of $2,000,000;
- failure to report a large cash transaction or an electronic funds transfer — a fine of $500,000 for a first offence and $1,000,000 for each subsequent offence;
- failure to retain records — up to five years imprisonment and/or a fine of $500,000; and
- failure to implement a compliance program — up to five years imprisonment and/or a fine of $500,000.

Effective December 30, 2008, failure to comply with the legislative requirements can also lead to the following administrative monetary penalties:

- failure to implement any of the elements of the compliance program could lead to an administrative monetary penalty of up to $100,000 for each one;
- failure to report the required information to senior management within 30 days after the review of the compliance program could lead to an administrative monetary penalty of up to $100,000.
Chapter 3

SUSPICIOUS TRANSACTIONS

A transaction is suspicious where, in the course of conducting certain activities on behalf of a client, there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist financing offence.

REPORTING SUSPICIOUS TRANSACTIONS

Section 7 and Section 8 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) address the reporting of suspicious transactions. The form and manner of reporting are set out in the Suspicious Transactions Reporting Regulations (STRR). Guidance in applying those regulations is provided in FINTRAC Guideline 2: Suspicious Transactions.

Persons and entities subject to the PCMLTFA are required to report transactions to FINTRAC when there are reasonable grounds to suspect that the transactions are related to the commission of a money laundering offence or a terrorist activity financing offence, and to provide terrorist property reports to FINTRAC.

As explained in FINTRAC Guideline 2, “reasonable grounds to suspect” is determined by what is reasonable in the circumstances, including normal business practices and systems within a particular industry. A “money laundering offence” involves various acts committed with the intention to conceal or convert property or the proceeds of property (e.g. money) knowing or believing that these were derived from the commission of a designated offence. In this context, a “designated offence” means most serious offences under the Criminal Code or any other federal Act.

FINTRAC Guideline 2 further explains that “terrorist activity financing offences” make it a crime to knowingly collect or provide property, such as funds, either directly or indirectly, to carry out terrorist activities. This includes inviting someone else to provide property for this purpose. There are other offences associated with terrorist activities that are not specifically related to financing, such as participating in or facilitating terrorist activities, or instructing and harbouring terrorists. Suspicion that a transaction is related to a terrorist activity financing offence triggers a requirement to report the transaction to FINTRAC whether or not the transaction has been completed. A completed transaction is one that has occurred. An attempted transaction includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the client.

Under the STRR, accountants and accounting firms serving as financial intermediaries are subject to the *PCMLTFA*. These obligations apply to CAs and CA firms that engage in, or give instructions with regard to, certain activities. Those activities, as illustrated in Exhibit 3.1, provide the foundation for determining whether there is a legal obligation to report suspicious transactions to FINTRAC. It is important to note, however, that a legal obligation does not apply in respect of:

- audit, review or compilation engagements carried out in accordance with the recommendations set out in the *CICA Handbook*;
- CAs who are employees or agents of a person or entity covered by the *PCMLTFA*;
- CAs who are employees or agents of a person or entity (third party) not covered by the *PCMLTFA*.

When it is determined that the CA or CA firm has a legal obligation to report to FINTRAC, a process along the lines illustrated in Exhibit 3.2 will help to facilitate information gathering, decision making and reporting, if appropriate, to FINTRAC.

Key sections of the STRR are set out in Exhibit 3.3. They prescribe a specific time limit for reporting suspicious transactions (Section 9) and the format for reporting (Section 12) — reports must be submitted in electronic format where the reporting entity has the capability. They also acknowledge that certain information about the transaction may not be readily available but reasonable measures must be taken to obtain that information (Section 11).

### IDENTIFYING SUSPICIOUS TRANSACTIONS

Information on identifying and reporting suspicious transactions is available in *FINTRAC Guideline 2: Suspicious Transactions*. Appendix C lists common indicators that might be useful in assessing whether a transaction is suspicious and should be reported. The common indicators cover general matters, knowledge of money laundering reporting or record-keeping requirements, identity documents, cash transactions, economic purpose, transactions involving accounts, transactions involving areas outside Canada, and transactions related to offshore business activity.

*FINTRAC Guideline 2* also provides several lists of industry-specific indicators compiled in consultation with reporting entities, law enforcement agencies and international financial intelligence organizations. Exhibit 3.4 sets out suspicious transaction indicators for accountants to use. The indicators must be assessed in the context in which the transaction occurs. Each indicator may contribute to a conclusion that there are reasonable grounds to suspect that the transaction is related to money laundering or terrorist financing. On the other hand, they may offer no indication of money laundering or terrorist activity financing in view of factors such as the client’s occupation, business, financial history and past investment pattern.

---

32 STRR Section 6(1), as amended.
33 Although a legal obligation may not exist, there may still be a moral or ethical obligation under the Rules of Professional Conduct to report such transactions with respect to illegal acts.
34 STRR Section 6(3), as amended.
35 STRR Section 6(2), as amended.
36 Exhibit 2.1 lists the pertinent Sections of the *Act* and Suspicious Transactions Reporting Regulations including the reporting of terrorist property.
Exhibit 3.1

Obligation to Report Suspicious Transactions to FINTRAC

Are you an “accountant” (CA) or “accounting firm” (CA firm)?

Yes →

On behalf of any person or entity, are you engaging in or giving instructions with respect to any of the following activities:
- receiving or paying funds?
- purchasing or selling securities, real property or business assets or entities?
- transferring funds or securities by any means?

No →

Yes →

Is there an attempted suspicious transaction or a completed suspicious transaction in respect of the activity?

No →

Yes →

The suspicious transaction must be reported to FINTRAC.

There is no obligation to report to FINTRAC.
Exhibit 3.2

Illustrative Process for Reporting a Suspicious Transaction

<table>
<thead>
<tr>
<th>Employee of accounting firm</th>
<th>Accountant responsible for engagement</th>
<th>Accountant other than responsible accountant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee encounters facts that constitute reasonable grounds to suspect a transaction is related to money laundering or terrorist activity financing</td>
<td>Responsible accountant encounters facts that constitute reasonable grounds to suspect a transaction is related to money laundering or terrorist activity financing</td>
<td>Accountant encounters facts that constitute reasonable grounds to suspect a transaction is related to money laundering or terrorist activity financing</td>
</tr>
<tr>
<td>Employee reports to the responsible accountant</td>
<td>Responsible accountant advises Compliance Officer of possible suspicious transaction</td>
<td>Accountant reports to the responsible accountant</td>
</tr>
<tr>
<td>Responsible accountant reviews facts and grounds for suspicion with Compliance Officer and any employee or accountant involved</td>
<td>Responsible accountant and Compliance Officer determine whether a report must be made</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Responsible accountant and Compliance Officer document reasons why a report is not required and place in the Compliance File</td>
<td>Responsible accountant and Compliance Officer prepare suspicious transaction report, submit to FINTRAC within 30 days and place a copy in the Compliance File</td>
<td></td>
</tr>
</tbody>
</table>

The Canadian Institute of Chartered Accountants
June 2008
Exhibit 3.3

Suspicious Transactions Reporting Regulations (STRR)

Section 2 — Interpretation
For the purposes of these Regulations, a person acting on behalf of their employer is considered to be acting on behalf of another person or entity except when the person is depositing cash into the employer’s account.

Section 6 — Application of Part 1 of the Act (wording identical to Part 1 Regulations, Section 34)

Section 9 — Reporting of Suspicious Transactions
(1) Subject to section 11, a report under section 7 of the Act concerning a financial transaction in respect of which there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering offence or a terrorist activity financing offence shall contain the information set out in Schedule 1.
(2) The report shall be sent to the Centre within 30 days after the person or entity or any of its employees or officers first detects a fact respecting a transaction that constitutes reasonable grounds to suspect that the transaction is related to the commission of a money laundering offence or a terrorist activity financing offence.

Section 10 — Report Made Under Section 83.1 of the Criminal Code
Subject to section 11, a report made under section 7.1 of the Act shall be sent without delay to the Centre and shall contain the information set out in Schedule 2.

Section 11 — Exemption
The requirement to report information set out in Schedule 1 or 2 does not apply to a person or entity in respect of information set out in an item of that Schedule that is not marked with an asterisk if, after taking reasonable measures to do so, the person or entity is unable to obtain the information.

Section 12 — Sending
(1) The report referred to in section 9 shall be sent electronically in accordance with guidelines for report submissions that are prepared by the Centre if the sender has the technical capabilities to do so.
(2) The report referred to in section 9 shall be sent in paper format in accordance with guidelines for report submissions that are prepared by the Centre if the sender does not have the technical capabilities to send the report electronically.
(3) The report referred to in section 10 shall be sent in paper format in accordance with guidelines for report submissions that are prepared by the Centre.

With respect to knowledge of the client’s business affairs, the “know your customer” concept is a requirement for complying with Canadian anti-money laundering laws. The most practical way to comply is to know your customer’s normal business activity so that suspicious or abnormal transactions can be recognized.

The “know your customer” approach has been a fundamental Canadian banking practice for many years. Since 1990, policy guidelines issued by the Office of the Superintendent of Financial Institutions (OSFI) titled “Deterring and Detecting Money Laundering” have required banks in Canada to identify and document transactions that were “of a suspicious nature.”
Exhibit 3.4

Suspicious Transactions Indicators for Accountants

To help identify suspicious transactions, CAs acting as financial intermediaries on behalf of a client should consider the following indicators:

- Client appears to be living beyond his or her means.
- Client has business activity inconsistent with industry averages or financial ratios.
- Client has cheques inconsistent with sales (i.e., unusual payments from unlikely sources).
- Client has a history of changing bookkeepers or accountants yearly.
- Client is uncertain about location of company records.
- Company carries non-existent or satisfied debt that is continually shown as current on financial statements.
- Company has no employees, which is unusual for the type of business.
- Company is paying unusual consultant fees to offshore companies.
- Company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues without reasonable explanation of the continued loss.
- Company shareholder loans are not consistent with business activity.
- Examination of source documents shows misstatements of business activity that cannot be readily traced through the company books.
- Company makes large payments to subsidiaries or similarly controlled companies that are not within the normal course of business.
- Company acquires large personal and consumer assets (i.e., boats, luxury automobiles, personal residences and cottages) when this type of transaction is inconsistent with the ordinary business practice of the client or the practice of that particular industry.
- Company is invoiced by organizations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven.  

FINTRAC Guideline 2 is not a substitute for the CA’s own assessment, based on knowledge, experience and the specific circumstances of the financial transaction. A suspicious transaction may involve several factors that may seem individually insignificant, but together may raise suspicion that the transaction is related to the commission of a money laundering offence or a terrorist activity financing offence. As a general guide, a transaction may be connected to money laundering or terrorist activity financing if it raises questions or gives rise to discomfort, apprehension or mistrust, regardless of the sum of money involved. Accordingly, there is no monetary threshold for making a report to FINTRAC on a suspicious transaction.

PREPARING AND TRANSMITTING REPORTS

Under STRR subsection 9(2), persons and entities must send the suspicious transaction report, containing the information set out in Schedule 1 of the Regulations, to FINTRAC within 30 days after detecting a fact related to a transaction that constitutes reasonable grounds to suspect that the transaction is related to the commission of a money laundering offence.

37 The OECD web site (www.oecd.org) lists non-cooperative countries with inadequate money laundering laws, that have highly secretive banking systems and that serve as corporate tax havens.
Instructions for preparing suspicious transaction reports are available in FINTRAC Guideline 3A: Submitting Suspicious Transaction Reports to FINTRAC Electronically and FINTRAC Guideline 3B: Submitting Suspicious Transaction Reports to FINTRAC by Paper. FINTRAC requires suspicious transactions reports to be prepared online, where the reporting person or entity has the technical capability to report electronically.

REPORTING TRANSACTIONS RELATED TO TERRORIST PROPERTY
With respect to property owned or controlled by or on behalf of a terrorist or a terrorist group, FINTRAC Guideline 2 notes that terrorist property must be frozen under the United Nations Suppression of Terrorism Regulations as well as the Anti-Terrorism Act additions to the Criminal Code. Therefore, the suspicious transaction should not be completed if the property in question is owned or controlled by or on behalf of a listed person or listed entity; that is, someone believed to be involved in terrorist activity. As part of international efforts to combat terrorism, the Government of Canada has published lists to prevent and suppress the financing of terrorist activities.\(^\text{38}\)

FINTRAC Guideline 5: Submitting Terrorist Property Reports explains reporting timelines, how reports have to be sent to FINTRAC, and what information has to be included in these reports. In addition to making a terrorist property report to FINTRAC, there is also a requirement under the Criminal Code for anyone in Canada and any Canadian outside Canada to disclose, to the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS), the existence of property in their possession or control that they know is owned or controlled by or on behalf of a terrorist or a terrorist group. Further information is provided in FINTRAC Guideline 1: Backgrounder and FINTRAC Guideline 5, Section 2.1.

KEEPING RECORDS OF SUSPICIOUS TRANSACTIONS
The Regulations require that records be kept for either attempted or completed suspicious transactions. Such records may help to demonstrate compliance, if the issue arises. From a practical perspective, it makes sense to implement a simple paper-based system for dealing with suspicious transactions. Consideration should also be given to establishing procedures for maintaining a compliance records file that is physically separate from client files. It could contain staff memos to supervisors, reporting worksheets and other records and documents pertaining to compliance. For this purpose, the FINTRAC paper-based suspicious transaction reporting form has all potentially reportable information presented in a manner that is essentially identical to the electronic reporting form.

LEGAL LIABILITY AND CLIENT COMMUNICATIONS

Under Part 5, Section 75(1) of the PCMLTFA, a financial intermediary that knowingly contravenes section 7 or section 7(1) by failing to report a suspicious transaction or to make a terrorist property report is guilty of an offence and liable on summary conviction for a first offence to a fine of up to $500,000 or imprisonment of up to six months, or both. A subsequent offence could result a fine of up to $1,000,000 or imprisonment of up to one year, or both. On conviction on indictment, a fine of up to $2,000,000 or imprisonment of up to five years, or both, may be imposed. Failure to keep records or identify clients can also lead to an administrative monetary penalty.

Part 5, Section 75(2) of the PCMLTFA offers a defence for employees by stating: “no employee of a person or an entity shall be convicted of an offence under subsection (1) in respect of a transaction or proposed transaction that they reported to their superior or in respect of property whose existence they reported to their superior.” Accordingly, employees who report suspicious transactions to their superior cannot be held liable for failing to report the suspicious transactions to FINTRAC. Part 1, Section 10 further states that those who make a suspicious transaction report in “good faith” are protected from criminal or civil proceedings.

On a final note, it is important to remember that the PCMLTFA states, in Part 1, Section 8, that no person or entity shall disclose that they have made a suspicious report to FINTRAC under Section 7, or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun. A conviction for tipping off a client that a report has been made could result in up to two years in prison (Part 5, Section 76 of the PCMLTFA).

The requirement to report suspicious transactions and the related disclosure prohibition have potential for placing a reporting CA or CA firm in conflict with the client, and in breach of the Rules of Professional Conduct. Consequently, this issue is discussed further in Chapter 6 of this Guide under Complying with the Rules of Professional Conduct.
Chapter 4

PREScribed TRANSACTIONS

A “prescribed transaction” is any transaction involving $10,000 or more in cash arising in the course of conducting certain activities on behalf of a client.

REPORTING PRESCRIBED TRANSACTIONS

“Prescribed financial transactions” encompass large cash transactions and electronic funds transfers. Under Section 9 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), “every person or entity referred to in section 5 shall report to the Centre, in the prescribed form and manner, every prescribed financial transaction that occurs in the course of their activities.” The form and manner of reporting are set out in detail in the Part 1 Regulations. 39

Under Section 34 of the Regulations, accountants and accounting firms serving as financial intermediaries are subject to the PCMLTFA. This applies to CAs and CA firms that engage in, or give instructions, with regard to certain activities. Those activities, as illustrated in Exhibit 4.1, provide the foundation for determining whether there is a legal obligation to report large cash transactions to FINTRAC. It is important to note, however, that a legal obligation does not apply40 in respect of:

- audit, review or compilation engagements carried out in accordance with the recommendations set out in the CICA Handbook.41
- CAs who are employees or agents of a person or entity covered by the Act.42
- CAs who are employees or agents of a person or entity (third party) not covered by the Act.

PREPARING AND TRANSMITTING REPORTS

CAs and CA firms that serve as financial intermediaries are required to report the following financial transactions:43

- large cash transactions involving amounts of $10,000 or more;
- sending or receiving of international electronic funds transfers of $10,000 or more;
- foreign exchange transactions at a rate that exceeds the posted rate, and the payment by an individual of transaction fees that exceed the posted fees.

---


40 Although a legal obligation may not exist, there may still be a moral or ethical obligation under the Rules of Professional Conduct to report such transactions with respect to illegal acts.

41 Part 1 Regulations, Section 34(3).

42 STR Regulations, Section 6 and Part 1 Regulations, Section 34(2).

43 Part 1 Regulations, Section 78(2).
Exhibit 4.1

Obligation to Report Large Cash Transactions to FINTRAC

Are you an “accountant” (CA) or “accounting firm” (CA firm)?

Yes →

On behalf of any person or entity, are you engaging in or giving instructions with respect to any of the following activities:
- receiving or paying funds?
- purchasing or selling securities, real property or business assets or entities?
- transferring funds or securities by any means?

Yes →

Is there a single transaction or a series of transactions in 24 hours with a total of $10,000 or more in respect of the activity?

Yes →

Is the cash received from a source other than a financial entity or a public body?

Yes →

The large cash transaction must be recorded and reported to FINTRAC.

No →

There is no obligation to report to FINTRAC.

No →

No →

No →

No
In determining the amount of a cash transaction that is not in Canadian dollars, Section 2 of the Regulations states: “Where a transaction is carried out by a person or entity in a foreign currency, the amount of the transaction shall, for the purposes of these Regulations, be converted into Canadian dollars based on:

(a) the official conversion rate of the Bank of Canada for that currency as published in the Bank of Canada’s Daily Memorandum of Exchange Rates that is in effect at the time of the transaction; or

(b) if no official conversion rate is set out in that publication for that currency, the conversion rate that the person or entity would use for that currency in the normal course of business at the time of the transaction.

According to Section 35 of the Part 1 Regulations, financial intermediaries must report to FINTRAC cash amounts of $10,000 or more received in the course of a single transaction, together with the information set out in Schedule 1. Schedule 1 of the Regulations identifies the types of data to be reported with respect to the following matters: the place of business where the transaction occurred; the transaction; account information; information on the person conducting the transaction; and information about the person or entity on whose behalf the transaction is conducted. The requirement to report does not apply if the cash is received from a financial entity or a public body. Also, certain information need not be reported if, after taking reasonable measures, the person or entity is unable to obtain the information.

The format for reporting is prescribed in Section 4 of the Part 1 Regulations — reports must be submitted in electronic format where the reporting entity has the capability. The reporting time limits are set out in Section 5 as follows:

- a report in respect of an electronic funds transfer must be sent to FINTRAC not later than five working days after the day of the transfer.
- a report in respect of a large cash transaction must be sent to FINTRAC within 30 days after the transaction, where the transaction occurs within 12 months after the coming into force of this section, or, in any other case, within 15 days after the transaction.

Instructions for preparing large cash transaction reports and electronic funds transfer reports are available in FINTRAC Guideline 7: Submitting Large Cash Transaction Reports to FINTRAC and FINTRAC Guideline 8: Submitting Electronic Funds Transfer Reports to FINTRAC.

---

44 Section 3 of the Part 1 Regulations states: “…two or more cash transactions or electronic funds transfers of less than $10,000 each that are made within 24 consecutive hours and that total $10,000 or more are considered to be a single transaction of $10,000 or more if:
(a) where a person is required to keep a large cash transaction record or to report an electronic funds transfer in accordance with these Regulations, the person knows that the transactions or transfers are conducted by, or on behalf of, the same person or entity; and
(b) where an entity is required to keep a large cash transaction record or to report an electronic funds transfer in accordance with these Regulations, an employee or a senior officer of the entity knows that the transactions or transfers are conducted by, or on behalf of, the same person or entity.

45 Section 1 of the Part 1 Regulations states that a financial entity means a bank, credit union, caisse populaire, a trust and loan company or an agent of the Crown that accepts deposit liabilities. A public body means a provincial or federal department or Crown agency, an incorporated municipal body (such as a city or town) and a hospital authority.

46 Part 1 Regulations, Section 52(1).
KEEPING RECORDS OF LARGE CASH TRANSACTIONS
CAs and CA firms that serve as financial intermediaries are required to:^47

- keep a large cash transaction record in respect of every amount in cash of $10,000 or more that they receive in the course of a single transaction, unless the cash is received from a financial entity or a public body (Section 36);
- ascertain the identity of the person involved in the transaction (Section 53);
- take reasonable measures to determine whether the individual who in fact gives the cash in respect of which the record is kept is acting on behalf of a third party (Section 8(1));
- keep a record when the individual is acting on behalf of a third party (Section 8(2)), or if there are reasonable grounds to conclude this is the case (Section 8(3)).

Depending on the type of activities they are involved in, financial intermediaries may also have to report the following financial transactions:

- the sending/receiving of international electronic funds transfers of $10,000 or more through the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network;
- other international electronic funds transfers of $10,000 or more through non-SWIFT networks.

Under Section 36 of the Regulations, financial intermediaries must “keep a large cash transaction record in respect of every amount in cash of $10,000 or more that they receive in the course of a single transaction.” According to Section 52(2), however, that requirement does not apply if such information is readily obtainable from other records that the person or entity must keep or retain under these Regulations.

Section 68 notes that persons and entities can keep records in a machine-readable form (on paper), or in electronic form, as long as a paper copy can be readily produced. For records that are kept electronically, an electronic signature of any individual required to sign the record must also be retained. Under Section 69, records must be retained for a period of five years from the day they were created or, in some cases, from the date the transaction was completed. Furthermore, Section 70 stipulates that records are to be kept in such a way that they can be provided to FINTRAC within 30 days of a request to examine them.

The required information and supporting documentation for these records and statements is specified in FINTRAC Guideline 6: Record Keeping and Client Identification. There are different versions of the Guideline, by sector. The following is an overview of the requirements.

Large cash transaction record (LCTR)
Section 6 of the PCMLTFA establishes duties for record keeping in accordance with the Regulations. Section 1(2) of the Part 1 Regulations indicates that a large cash transaction record (LCTR) must contain the following:

- the name of the individual who in fact gives the amount;
- the individual’s address and nature of principal business or occupation;

---

47 Part 1 Regulations, Section 78(1) states that the regulations come into force on June 12, 2002, subject to subsection (2) which specifies the provisions that come into force on January 31, 2003 and the provisions that come into force on March 31, 2003.
• date, time and nature of the transaction;
• number of any account affected by the transaction, the type of account, the full name of any person or entity that holds the account, and the currency in which the account transaction is conducted;
• the purpose and details of the transaction, including other persons or entities involved and the type of transaction (such as cash, electronic funds transfer, deposit, currency exchange or the purchase or cashing of a cheque, money order, traveller’s cheque or banker’s draft);
• whether cash is received by armoured car, in person, by mail or any other way; and
• the amount and currency received.

It is important to note that a copy of the LCTR is not sufficient for reporting a large cash transaction to FINTRAC because the data required for that report are different from those required for the LCTR.

Identity of person or entity involved in a large cash transaction
Under Section 53 of the Part 1 Regulations, financial intermediaries involved in a large cash transaction are required to ascertain the identity of the person making that transaction. For a transaction involving an individual (Section 64(1)(d)), this must be done at the time of the transaction (Section 64(2)(b)), by reference to any of the following original documents (Section 64(3)):
• birth certificate;
• driver's licence;
• provincial health insurance card (except where such use contravenes provincial legislation);
• passport; or
• any similar record.

For a transaction involving a corporation, its existence, name and address and the names of its directors must be ascertained by referring to its certificate of corporate status or annual records (Section 65). For a transaction involving an entity other than an individual or corporation, its existence must be ascertained by referring to partnership agreements, articles of association or other similar record that ascertains its existence (Section 66).

Once the identity is ascertained in accordance with Sections 64, 65 or 66, there is no further requirement to ascertain that same identity again (Section 63). Nonetheless, a record of the type and source of the record consulted, or a paper copy of that record must be retained. In addition, under Section 67, the LCTR must note the:
• date of birth of the person;
• type and reference number of the record used to ascertain the identity of the person;
• place where the record was issued.
Acting on behalf of a third party
Section 8(1) of the Part 1 Regulations states that every person or entity that is required to keep a large cash transaction record must “take reasonable measures to determine whether the individual who in fact gives the cash in respect of which the record is kept is acting on behalf of a third party.” There is no specific direction provided, however, as to what constitutes “reasonable measures” and this could differ from one situation to another.

Third party disclosure statement
According to Section 8(2) of the Part 1 Regulations, where the person or entity determines that the individual is acting on behalf of a third party, a record must be kept that sets out the following:
- if the third party is an individual, the third party’s name, address and the nature of the principal business or occupation of the third party;
- if the third party is an entity, the third party’s name, address and the nature of the principal business of the third party; if the entity is a corporation, the entity’s incorporation number and its place of issue; and
- the nature of the relationship between the third party and the individual who gives the cash.

According to Section 8(3), where the person or entity is not able to determine whether the individual is acting on behalf of a third party but there are reasonable grounds to suspect that the individual is doing so, a record must be kept that:
- indicates whether, according to the individual, the transaction is being conducted on behalf of a third party; and
- describes the reasonable grounds to suspect the individual is acting on behalf of a third party.

Receipt of funds record
Recent amendments to the Regulations state that a receipt of funds record must be prepared for any amount of $3,000 or more, whether or not it is received in cash. However, there is no need to keep a receipt of funds record:
- if a large cash transaction record has already been prepared for the same transaction;
- if the funds are received from a financial entity or a public body;
- if the funds are for the payment of professional fees; or
- if the information is readily available in other records that are maintained.

FINTRAC Guideline 6D, Record Keeping and Client Identification for Accountants states that, for any receipt of funds of $3,000 or more, the following information is required:
- the amount and currency of the funds received;
- the date of the transaction;
- the purpose, details and type of transaction (for example, the funds were for you to transfer on your client’s behalf, etc.), including whether any other individuals or entities were involved in the transaction;
- if the funds received were cash, how the cash was received (for example, in person, by mail, by armoured car, or any other way); and
• if an account was affected by the transaction, the number and type of any such account, the full name of the client that holds the account; and the currency in which the transaction was conducted.

If the receipt of funds record is about an individual, it also has to include the name and address of the individual from whom the funds were received, that individual’s date of birth as well as that individual’s principal business or occupation. If the receipt of funds record is about an entity, it will have to include the entity’s name, address and nature of their principal business.

LEGAL LIABILITY AND CLIENT COMMUNICATIONS

Under Part 5, Section 77(1) of the PCMLTFA, financial intermediaries that fail to report a large cash transaction or an electronic funds transfer may be subject to criminal charges resulting in a fine of $500,000 for a first offence, and $1,000,000 for each subsequent offence. A failure to retain records may result in up to five years imprisonment, a fine of $500,000, or both (Section 74(b)). Failure to keep records or identify clients can also lead to an administrative monetary penalty.

Section 77(2) of the PCMLTFA provides that “no person or entity shall be convicted of an offence under subsection (1) if they exercised due diligence to prevent its commission.” It is also noteworthy that, under Section 10 of the PCMLTFA, anyone who makes a large cash transaction report in “good faith” is protected from criminal or civil proceedings.

Clearly, the requirements to record large cash transactions and the related information, and to report such transactions to FINTRAC, have potential for placing a reporting CA or CA firm in conflict with the client, and in breach of the Rules of Professional Conduct. Guidance on this issue, particularly with respect to client communications, is provided in Chapter 6 of this Guide under Complying with the Rules of Professional Conduct.
Chapter 5

CROSS-BORDER CURRENCY
AND MONETARY INSTRUMENTS

“Cross-border currency and monetary instrument transactions” involve the exporting or importing of $10,000 or more of cash or monetary instruments.

CROSS-BORDER CURRENCY AND MONETARY INSTRUMENT REPORTING (CCMIR)

To stem the physical flow of the proceeds of crime across Canada’s borders, Part 2 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) deals with Reporting of Currency and Monetary Instruments. Under Part 2, every cross-border transfer, including those by mail or courier, of any currency or any monetary instruments at or above an established threshold must be reported to the Canada Border Services Agency (CBSA). The regulatory regime is similar to the cross-border reporting requirements in the United States, and will complement current Canadian and US efforts to detect and deter money laundering and terrorist financing.

Unlike Part 1 of the PCMLTFA that applies only to specified persons and entities, Part 2 applies to all persons and entities including all CAs and CA firms, whether or not they serve as financial intermediaries on behalf of their clients. The form and manner of reporting under Part 2 of the PCMLTFA are set out in the “Cross-Border Currency and Monetary Instruments Reporting Regulations” (SOR/2002-412 and SOR/2003-358).

The CCMIR Regulations:

- define the term “monetary instruments” which includes, among other things, stocks, bonds, bank drafts and travellers’ cheques.
- establish the CCMIR threshold at $10,000 (Section 2(1) of the Regulations).
- prescribe (in Schedules 1, 2 and 3) the information to be included in the CCMIR reports.
- provide for exceptions from reporting (for example, where currency or monetary instruments are brought into Canada, but Canada is a transit point rather than the final destination).
- set at up to 30 days the period for which a customs officer is authorized to retain currency or monetary instruments that a person has declared, but for which a report is pending.

Although the CBSA has primary responsibility for administering the CCMIR Regulations, customs officers must send the CCMIR reports submitted to them to FINTRAC (Section 12(5) of Part 2 of the PCMLTFA). Furthermore, if a customs officer has reasonable grounds to suspect that information obtained while enforcing the PCMLTFA would assist in the detection, prevention or deterrence of money laundering or the financing of terrorist activities, the customs officer may disclose it to FINTRAC or law enforcement authorities (Section 36 of Part 2 of the PCMLTFA).
Under Part 2, Section 12 of the PCMLTFA, the obligation for reporting will rest with the originating exporter. Therefore, CAs and CA firms sending or “exporting” cash or monetary instruments of $10,000 or more across Canada’s borders, by mail or courier, will be required to complete a CCMIR report. Those receiving or “importing” such cash or monetary instruments will not be required to complete a CCMIR report, unless they receive a notice under Part 2, Section 14(2) of the PCMLTFA.

OPENING MAIL AND DISCLOSING INFORMATION
To enforce CCMIR obligations, Part 2, Section 17 of the PCMLTFA allows CBSA officers to “examine any mail that is being imported or exported, and open or cause to be opened any such mail that the officer suspects on reasonable grounds contains currency or monetary instruments” of a value equal to or greater than $10,000. These examinations will occur at central mail sorting facilities.

With three exceptions, Part 2, Section 36 of the PCMLTFA prohibits the disclosure of any information obtained from opening mail. Those exceptions allow disclosure to FINTRAC, to law enforcement, and any disclosure that may occur as CBSA officers exercise their powers, or perform their duties and functions, under Part 2 of the PCMLTFA. According to Section 36, it is not clear if it is only CCMIR report information that can be disclosed, or if any other information found can also be disclosed. It is CBSA’s position that this provision allows the disclosure to the noted entities of any information found in a mail item. The respective conditions and purposes for disclosure under Sections 36(2) and 36(3), however, are different. Section 36(2) appears to allow, at the sole discretion of a CBSA officer, direct disclosure to law enforcement, in certain specified circumstances, of any information found in a mail item. This bypasses the filtering and limited disclosure that would normally occur in the process FINTRAC is to follow in disclosing reported information to law enforcement authorities.

LEGAL LIABILITY AND CLIENT COMMUNICATIONS
Part 5 of the PCMLTFA provides for a maximum fine of $500,000 and a maximum jail term of five years for failure to cooperate with the customs officer when a report is submitted, such as answering truthfully any questions that the customs officer asks or opening any package or container that the officer wishes to examine. In addition, non-reported currency or monetary instruments are forfeited to the Crown. If there is no suspected link to money laundering or terrorist financing, the forfeited funds may be retrieved after payment of penalties from $250 to $5,000. CBSA will provide information and guidance on the reporting obligations via fact sheets, press releases, brochures, posters and postings on the CBSA Web site.

With respect to the requirements in Part 2, Section 12 of the PCMLTFA, it would be prudent for CAs and CA firms to advise their clients at the time the engagement is accepted that they may have a duty to report the importation or exportation of currency or monetary instruments of $10,000 or more. As well, the possibility that a CBSA officer could open mail sent to, or by, a CA or CA firm is an issue that may need to be disclosed to clients. Furthermore, in light of the requirements of Part 2, Section 36 of the PCMLTFA, it would be prudent for CAs and CA firms to advise their clients at the time the engagement is accepted that a CBSA officer could disclose any information found in a mail item. These matters are discussed further in Chapter 6 of this Guide under Complying with the Rules of Professional Conduct.
Chapter 6

RULES OF PROFESSIONAL CONDUCT

The Rules of Professional Conduct with respect to client confidentiality and association with unlawful activities are of particular relevance to the issue of money laundering.

COMPLYING WITH THE RULES OF PROFESSIONAL CONDUCT

Canada’s provincial Institutes of Chartered Accountants work in partnership to develop and enforce high national standards to protect the public interest and maintain the good reputation and integrity of the CA profession. The broad spectrum of standards, processes and activities to achieve these goals includes:

- nationally harmonized rules of professional conduct adopted as measures of self-governance by all chartered accountants, through their respective provincial institutes, which enforce them in accordance with their responsibilities as the CA profession’s governing bodies;
- in provinces other than Québec, Council Interpretations adopted by the councils of the provincial institutes to provide guidance in following the rules of professional conduct.

The Rules of Professional Conduct (Rules) are aimed, first and foremost, at the protection of the public, and secondly, at achieving orderly and courteous conduct between licensees. The Rules reflect a number of principles — fundamental statements of accepted conduct, the soundness of which is self-evident. Application of the Rules may also extend to activities that do not constitute public accounting. Of particular relevance to the issue of money laundering are the Rules with respect to the duty of confidence and association with unlawful activities.

DUTY OF CONFIDENCE

Under the Rules, CAs have a duty of confidence in respect of the affairs of each and every client and shall not normally disclose, without proper cause, any information obtained in the course of their duties, nor shall they in any way exploit such information to their advantage. In other words, practitioners shall not normally disclose any “confidential client information” concerning the business and affairs of a client, acquired in the course of a professional relationship with the client. Such information is confidential to the client regardless of the nature or source of the information or the fact that others may share the knowledge. Such information remains confidential until the client expressly or impliedly authorizes it to be divulged. In addition, practitioners shall not use any confidential information to the disadvantage of such client or employer without the knowledge and consent of the client.

---

48 Most of the Provincial Institutes/Ordre Rules of Professional Conduct are available online. See, for example, the Institute of Chartered Accountants of Ontario and the Institute of Chartered Accountants of BC.
49 Refer, in provinces other than Québec, to the glossary in the Council Interpretations.
Normally, the duty of confidence would preclude communication to a third party with respect to the activities of a client.\(^{50}\) Nonetheless, when a CA or CA firm serves as a financial intermediary on behalf of a client, they are required by statute to report suspicious transactions and large cash transactions of $10,000 or more. Furthermore, the \textit{PCMLTFA} states, in Section 8, that no person or entity shall disclose that they have made a suspicious report to FINTRAC under Section 7, or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun.\(^{51}\) A conviction for tipping off a client that a report has been made could result in up to two years in prison.

Although the requirements have potential for placing a reporting CA or CA firm in conflict with the client, it is clear that the specific statutory requirements override the general requirement to maintain confidentiality. In other words, a CA or CA firm will not be found in breach of the confidentiality \textit{Rules} where there is a statutory requirement to disclose information to third parties, such as FINTRAC and other regulators.\(^{52}\) This is an issue that CAs and CA firms should discuss with their clients.

In addition, to enforce CCMIR obligations, Section 17 of the \textit{PCMLTFA} allows CBSA officers to “examine any mail that has been imported or exported, and open or cause to be opened any such mail that the officer suspects, on reasonable grounds, contains currency or monetary instruments” of a value equal to, or greater than, $10,000. The possibility that a CBSA officer could open confidential mail sent to, or by, a CA or CA firm is another issue that CAs and CA firms should discuss with their clients.

In summary, a CA or CA firm serving as a financial intermediary on behalf of a client should develop a communications strategy to fully disclose, in writing, the reporting obligations and other requirements under the \textit{PCMLTFA}. An example of a communication letter to a client is provided in \textit{Exhibit 6.1}. The contents of the letter would be discussed with the client, and the client’s acknowledgement, preferably in writing, would be obtained. If the client does not give consent to proceed, the CA or CA firm should consider whether the engagement should be discontinued / not accepted.\(^{53}\)

\textbf{UNLAWFUL ACTIVITY}

The \textit{Rules} specifically address “Unlawful Activity” and establish the minimum level of ethical conduct for practitioners. In this regard, it is important to note that money laundering is an illegal activity and may also be connected with fraud. Therefore, CAs and CA firms must not knowingly lend themselves or their services to any such activity.\(^{54}\) They should be mindful of the possibility of money laundering and knowingly or unknowingly becoming a party to the offence under the \textit{Criminal Code} by failing to take appropriate action.\(^{55}\)

\(^{50}\) The requirement to keep a client’s affairs confidential should not be confused with the legal concept of “solicitor/client privilege.”
\(^{51}\) The requirement to report a suspicious transaction applies whether or not the transaction has been completed.
\(^{52}\) Refer, in provinces other than Québec, to Council Interpretation of Rule 208.1 on “Confidentiality of Information.”
\(^{53}\) Refer to Rule 204.8 on “Disclosure of Impaired Independence.”
\(^{54}\) Refer to Rule 213 on “Unlawful Activity.”
\(^{55}\) When faced with such conflicts, practitioners should seek legal advice.
Exhibit 6.1

Communication Letter to Clients on Money Laundering Obligations

Date: ____________

Dear [name of client]:

Re: Proceeds of Crime (Money Laundering) and Terrorist Financing Act

New Legislation to Combat Money Laundering and Terrorist Financing

The Canadian federal government has enacted the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act). The Act implements specific measures to detect and deter money laundering and terrorist financing activities and to facilitate the investigation and prosecution of money laundering and terrorist financing offences.

Certain professionals, including chartered accountants, are subject to mandatory reporting, record keeping and client identification requirements. In particular, CAs and CA firms that serve as financial intermediaries on behalf of their clients must now keep detailed records and report selected information on certain client transactions to an anti-money laundering agency, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

New Reporting Obligations

The legislation requires CAs and CA firms that serve as financial intermediaries to report “suspicious transactions,” that is, financial transactions we reasonably suspect are related to the commission of a money laundering or terrorist financing offence. The Act specifically prohibits CAs and CA firms from informing a client that a suspicious transaction report has been made, or from disclosing to a client the contents of a report. Other provisions of the Act impose further legal obligations on us:

- to report large cash transactions of $10,000 or more;
- to keep a record of large cash transactions for five years; and
- to report the cross-border movement of currency and monetary instruments of $10,000 or more.

Under provisions of the Act, certain authorities will have the power to enter our premises, without a search warrant, to determine if we are complying with the Act. In this regard, FINTRAC officials will be able to access our computer and data processing system, examine and copy file information and records, and reproduce any information or record. In addition, the Canada Border Services Agency will have the authority to seize, retain and open mail that it reasonably believes contains $10,000 or more in cash or monetary instruments.

Disclosing Confidential Client Information

The Rules of Professional Conduct for CAs and CA firms establish a duty of confidence that obliges us to keep confidential all information about the business and affairs of our clients, unless our clients authorize us to release the information or we are required by law or a court to do so. The Proceeds of Crime (Money Laundering) and Terrorist Financing Act requires us, by lawful authority, to disclose certain client information. Nonetheless, to comply with our duty of confidence, we will ensure that we report or record only the information that is required under the Act, and we will carefully comply with the prescribed form and manner of reporting and recording financial transactions.

Yours truly,

[Name of CA or CA firm]

Client Acknowledgement

I acknowledge that the contents of this letter have been discussed with me.

[Client signature and date]
Chapter 7

IMPLICATIONS FOR PRACTITIONERS INVOLVED IN AUDIT, REVIEW AND COMPILATION ENGAGEMENTS

Although the PCMLTFA does not apply to audit, review and compilation engagements, practitioners providing such services need to consider whether any responsibilities are imposed on them by the CICA Handbook – Assurance.

As noted in Chapter 1, the Part 1 Regulations to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) state that the Act “does not apply in respect of audit, review or compilation engagements carried out in accordance with the recommendations set out in the CICA Handbook.”56 Therefore, practitioners providing such services in Canada do not have a statutory reporting responsibility with respect to money laundering and terrorist financing activities.

Nevertheless, during the course of an audit, review or compilation engagement, practitioners may encounter circumstances where the proceeds of crime are, or may be, laundered. In such cases, they need to be aware of the appropriate action to take to avoid potentially serious consequences that may include:

- an increased risk of misstatement in the financial statements due to money laundering;
- an increased risk of other forms of fraud;
- a detrimental effect on the practitioner’s reputation; or
- potential adverse legal consequences for the practitioner.

AUDIT ENGAGEMENT CONSIDERATIONS

In Canada, money laundering is an illegal activity.57 Accordingly, practitioners providing audit services would be guided by the standards set out in the CICA Handbook – Assurance Section 5136, “Misstatements – Illegal Acts.” Section 5136 requires that practitioners apply their knowledge of the business and make enquiries of management to identify laws and regulations which, if violated, could reasonably be expected to result in a material misstatement in the financial statements.58

---

56 Identical wording is used in Part 1 Regulations, Section 34 (3) and Suspicious Transactions Reporting Regulations, Section 6(3).
57 In 1990, Canada passed legislation that identified money laundering as a criminal offence. Money laundering offences include illegal acts, such as drug trafficking, murder, robbery, bribery, fraudulent manipulation of stock exchange transactions, possessing, issuing or circulating counterfeit money, theft, extortion, forgery and fraud.
58 Refer to CICA Handbook – Assurance, paragraph 5136.11.
Anti-money laundering laws and regulations may be identified as a result of this process. In those situations where anti-money laundering laws and regulations are identified, practitioners would consider the likelihood of a violation of such laws when assessing inherent risk and would perform procedures the nature, extent and timing of which depend on the inherent risk of a material misstatement.

During the normal course of an audit engagement, practitioners could encounter circumstances that lead them to suspect that the financial statements are materially misstated as a result of the consequences of money laundering. Also, because money laundering is often connected with fraud, practitioners could encounter circumstances that indicate the financial statements may contain a material misstatement arising from fraud. In such cases, they should consider the implications for the engagement, including the need to reconsider planned procedures.

Normally, the communication of illegal acts to third parties is not the auditor’s responsibility. When there is evidence that money laundering or possible money laundering may have occurred, however, practitioners should ensure the audit committee or equivalent and appropriate levels of management are informed. Because the duty of confidentiality would usually preclude such communication, except in connection with the expression of an opinion on the financial statements, caution should be exercised in determining with whom to communicate. Where practitioners face conflicting responsibilities with respect to the communication of money laundering activities to third parties, they should consider seeking legal advice.

REVIEW ENGAGEMENT CONSIDERATIONS
Practitioners performing a review of financial statements would be guided by the standards set out in Handbook Section 8100, “General Review Standards” and Section 8200, “Public Accountant’s Review of Financial Statements.” In conducting a review, they would use procedures consisting primarily of enquiry, analysis and discussion. During the course of the review, if practitioners encounter circumstances that raise doubts about the plausibility of the financial statements with respect to the consequences or potential consequences of money laundering, they would consider performing additional procedures to address the doubts. Such procedures may be similar to those used on an audit, as previously discussed.

COMPILATION ENGAGEMENT CONSIDERATIONS
Practitioners performing a compilation of financial statements would be guided by the standards set out in Handbook Section 9200, “Compilation Engagements.” In this regard, paragraph 9200.18 states that when the public accountant is aware of matters that would cause the financial statements to be false or misleading, they should request additional or revised information. If management does not provide the information requested or does not agree with the statements, the public accountant should not release the statements and withdraw from the engagement.

---

59 Refer to CICA Handbook – Assurance Section 5135, “The Auditor’s Responsibility to Consider Fraud,” paragraphs 5135.42, 5135.43 and related Appendix C.

60 Refer to CICA Handbook – Assurance, paragraph 5136.30.
Appendix A

MONEY LAUNDERING METHODS AND EXAMPLES

This Appendix explains some common money laundering methods and provides a variety of illustrative case examples of money laundering.

COMMON MONEY LAUNDERING METHODS

Nominees
This is one of the most common methods of laundering and hiding assets. A launderer uses family members, friends or associates who are trusted within the community, and who will not attract attention, to conduct transactions on their behalf. The use of nominees facilitates the concealment of the source and ownership of the funds involved. CAs may be used unwittingly as nominees.

Structuring or “smurfing”
Many inconspicuous individuals deposit cash or buy bank drafts at various institutions, or one individual carries out transactions for amounts less than the amount that must be reported to the government, and the cash is subsequently transferred to a central account. These individuals, commonly referred to as “smurfs,” normally do not attract attention as they deal in funds that are below reporting thresholds and they appear to be conducting ordinary transactions.

Asset purchases with bulk cash
Individuals purchase big-ticket items such as cars, boats and real estate. In many cases, launderers use the assets but distance themselves by having the assets registered in the name of a friend or relative. The assets may also be resold to further launder the proceeds.

Exchange transactions
Individuals often use the proceeds of crime to buy foreign currency that can then be transferred to offshore bank accounts anywhere in the world.

Currency smuggling
Funds are moved across borders to disguise their source and ownership, and to avoid being exposed to the law and systems that record money entering into the financial system. Funds are smuggled in various ways (for example, by mail, courier and body-packing) often to countries with strict bank secrecy laws.
Gambling in casinos
Individuals bring cash to a casino and buy gambling chips. After gaming and placing just a few bets, the gambler redeems the remainder of the chips and requests a casino cheque.

Black-market peso exchange
An underground network of currency brokers with offices in North America, the Caribbean and South America allows drug traffickers to exchange pesos for US dollars. The dollars stay in the United States and are bought by South American (mainly Colombian) companies, which use them to buy American goods for sale back home.

ILLUSTRATIVE CASE EXAMPLES OF MONEY LAUNDERING

Use of Indirect Deposit Services
A small-time drug trafficker operating out of Vancouver had his wholesalers deposit money into his account using the multi-branch or “INTERAC” computerized bank tellers. He then withdrew the money to purchase money orders in US funds. These money orders were subsequently sent to South America to purchase drugs or to Greece to be repatriated at a later date.

Immediate Withdrawal
A Montreal area man made his first cash deposit from the proceeds of drug trafficking. Over the next three weeks, he deposited $3.7 million. In the next three months, he made 20 deposits for a total of $8 million. In every instance, right after depositing the money, the man immediately withdrew it in the form of a bank draft signed by the assistant manager of the deposit-taking institution. The drafts were later deposited in banks in Switzerland, Italy and Spain.

Negotiable Instruments
A money launderer for a major drug trafficking organization laundered over $4 million (CDN) through a Vancouver branch of a Schedule II bank. Over eight months, nine bank drafts were purchased by the launderer or his “smurfs.” The average value of each bank draft was over $450,000. The majority of these bank drafts would be cashed at a bank in Luxembourg.

Electronic Wire Transfers
From a branch of a Schedule II bank in Vancouver, a launderer for an international drug trafficking ring wire transferred funds to three different banks in Japan. Part of the money then went to Thailand to purchase heroin. In all, $302,000 out of $563,000 identified by police as the proceeds of crime was laundered via this route.

Denomination Exchange
A Winnipeg resident owned a local car dealership and was also suspected of being involved in the local drug trade. He was observed travelling from bank to bank with known drug traffickers. Small denominations of cash were converted to larger bills that he used to purchase houses, cars and race horses.
Conversion into U.S. Currency
A lawyer was used by drug traffickers to launder cash through local banks. The lawyer’s role was to take Canadian cash from the dealers to a Schedule II bank in Vancouver. The cash would then be exchanged for American currency. Over a four-month period, the lawyer exchanged a total of $3.1 million from Canadian currency into US funds on 18 occasions, with amounts ranging from $56,000 to $396,000.

Bank Loans
A Canadian landed immigrant who had resided in California for a number of years returned to Winnipeg and opened a bank account by depositing two U.S. bank drafts for $12,000. He also deposited $10,000 (US) in cash in the form of $50 bills. Shortly after opening this account, he approached the bank about taking out a loan for $11,000 to pay off a US loan currently on his automobile. The loan was denied.

It is suspected that the individual was attempting to substitute part of the illicit funds brought into Canada by way of the Canadian bank loan. It is believed that once the loan was obtained, the subject would have paid off both the US loan and then the Canadian loan. He would then be able to sell the vehicle (a BMW) and deposit the “clean” money into the bank.

Bank Performing Transaction on Behalf of Customer
The Supreme Court of Ontario froze $13.5 million (US) in the account of a branch of a Schedule II bank. The account itself was registered in the name of a Panamanian Bank. Drug Enforcement Administration (DEA) officials in the US allege that the Panamanian Bank arranged the electronic wire transfer of the money into an account of the Schedule II bank.

Discretion of Bank Staff
An organized crime syndicate laundered the illicit proceeds of its drug trafficking business by making cash deposits once, twice or three times a week, predominately in one account at a branch of a Montreal bank. Total cash deposits amounted to $13 million dollars (US). In one month alone, a single deposit of $1.2 million was made. The amount of money being laundered was so great that cash would be stuffed into tote bags, loaded onto pick-up trucks and backed up to the front door of the branch.

Through the bank in Montreal, the group laundered $14 million over an eleven-month period. The cash was brought to the bank in suitcases or paper bags. So much cash was deposited that the bank requested it be organized in bundles of $5,000 before being brought in. The request was complied with and the bank accepted these large cash deposits without question and even created a special account for the customer.
Tax Havens
A cocaine and marijuana smuggler from Florida is believed by the US Federal Bureau of Investigation (FBI) to have laundered approximately $100 million (US) a year over a 6 year period. He would deposit the cash into a branch of a Canadian bank located in Nassau, Bahamas. Several accounts would be used, all of them in the name of Nassau-registered corporations. The money was then wired to the bank's Cayman Islands branch and into the account of a company. From there the money was wired back to the United States into the bank's New York City branch. It would then be dispersed among numerous corporations owned by the individual in the US.

Insurance Policy
An individual was convicted of stealing over $100,000 from two charitable organizations. During the course of the investigation, police learned that the accused was the owner of a fully paid annuity policy having a value of $140,000. The annuity had been purchased from a Canadian life insurance company. It was later ruled that a portion of the money invested in the annuity was the proceeds of the original crime.

Money Laundering and Fraud
In March 2000, an insurance company executive embezzled $90 million by faking the purchase of bonds as an investment for his employer. To conceal the funds’ movement, he arranged for them to be passed first through two companies an accounting firm had set up for him in a Caribbean nation and then to his personal account in a third jurisdiction. Six months later, the accounting firm detected the executive’s fraud and its inadvertent role in laundering the proceeds. Nevertheless, the firm’s management committee did not report its findings to the authorities and later both they and the executive were apprehended and charged for their offenses. (Source: FATF Report on Money Laundering Typologies, 2000-2001)

Sanitized Money Laundering Cases
To show how complex and tangled money laundering schemes can be, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has prepared a link chart of a money laundering case, with details changed or deleted for security and privacy reasons. The Egmont Group has also prepared a Library of Sanitized Cases, including a compilation of 100 sanitized cases on successes and learning moments in the fight against money laundering.\(^{61}\)

\(^{61}\) The FINTRAC sanitized money laundering case is available online (http://www.fintrac.gc.ca/fintrac-canafe/hfbac-eng.asp). The Egmont Group’s Library of Sanitized Cases is also available online (http://www.egmontgroup.org/library_sanitized_cases.html).

The Canadian Institute of Chartered Accountants

June 2008
Appendix B

INTERNATIONAL MONEY LAUNDERING DEVELOPMENTS

This appendix reviews money laundering developments from an international perspective. It covers joint initiatives by the Financial Action Task Force as well as initiatives by Australia, the United Kingdom, the United States, New Zealand and the International Federation of Accountants.

Joint International Initiatives
Money laundering is a global phenomenon that is facilitated by the increasingly international character of business, financial and criminal activity.\(^\text{62}\) To help disguise the origins of the proceeds of crime, money laundering often involves the international movement of those proceeds. This disrupts financial systems around the world by damaging the reputation of international financial institutions and weakening their relationships with intermediaries, regulators and the general public.

One of the first highly publicized global money laundering operations was the Bank of Commerce and Credit International (BCCI). In 1988, BCCI was the seventh largest private bank in the world, with approximately $20 billion in assets. It had headquarters in Luxembourg and 400 branches in 72 countries. Money laundering perpetrators bought BCCI certificates of deposit in six countries with drug money and then used them as collateral for loans. Because jurisdictional boundaries made international law enforcement difficult, it was acknowledged that international cooperation was essential to the deterrence, detection and prosecution of money laundering.

International organizations, such as the United Nations and the Bank for International Settlements, took initial steps in the late 1980s to address the money laundering problem. To coordinate an international response, the Group of Seven (G-7) formed the Financial Action Task Force on Money Laundering (FATF) in 1989.\(^\text{63}\) In 1990 the FATF issued a report containing 40 recommendations — addressing the criminal justice system and law enforcement, the financial system and its regulation, and international cooperation — to help combat money laundering.\(^\text{64}\)


\(^\text{63}\) The Group of Seven (G7) initially included Canada, France, Germany, Italy, Japan, the United Kingdom and the United States. It now comprises more than 30 countries, jurisdictions, and intergovernmental organizations.

\(^\text{64}\) The FATF 40 + 9 Recommendations and its Methodology for Assessing Compliance are on the Internet (http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236920_1111111100.html).
The FATF Recommendations have been endorsed by more than 130 countries, are widely accepted as the leading international anti-money laundering standard, and have been, or are being, successfully implemented. However, money laundering methods and techniques change as new measures to combat money laundering are implemented and new technologies are developed.

The FATF identified a number of areas where possible changes could be made to the FATF framework, and these were set out in the “Review of the FATF Forty Recommendation Consultation Paper” published in May 2002. The broad topics covered include customer due diligence and suspicious transaction reporting, beneficial ownership and control of corporate vehicles, and the application of anti-money laundering obligations to non-financial businesses and professions. Each topic sets out the nature of the problem or issue, identifies the risks, outlines the current position, and provides one or more options or alternatives for dealing with the issue or risks. After broad consultation, the revised FATF 40 Recommendations (2003) were published.

After the tragic events in the United States on September 11, 2001, a number of governments called for a rapid and coordinated effort to detect and prevent the misuse of the world financial system by terrorists. At a special meeting in October 2001, the FATF expanded its mission beyond money laundering to focus its energy and expertise on the worldwide effort to combat terrorist financing. In this regard, the FATF has issued new international standards to combat terrorist financing which the Task Force calls on all countries to adopt and implement. Implementing these Special Recommendations on Terrorist Financing will deny terrorists and their supporters access to the international financial system.

Annually, FATF experts meet to discuss money laundering methods and trends. This provides a venue for law enforcement and regulatory experts to identify and describe current money laundering methods and trends, emerging vulnerabilities and potential counter-measures. The FATF Typologies Reports cover matters such as the following:

- online banking and internet casinos;
- trust, other non-corporate vehicles and money laundering;
- lawyers/notaries, accountants and other professionals;
- the role of cash versus other payment methods in money laundering schemes;
- terrorist related money laundering;
- terrorist financing;
- coordinated money laundering among organized crime groups;
- suspicious transaction reports (STRs) and money laundering cases;
- money laundering through the securities sector;
- the gold and diamond markets;
- insurance and money laundering;
- credit and debit cards and money laundering.
During 2006-2007, the FATF explored a number of money laundering and terrorist financing methods and techniques, producing six studies on key areas: trade-based money laundering; new payment methods; misuse of corporate vehicles; money laundering associated with VAT carousel fraud; laundering the proceeds of illegal narcotics trafficking; and money laundering and terrorist financing through the real estate sector.\(^{65}\)

In 2008, the UK Chancellor of the Exchequer chaired a meeting of FATF Ministers in Washington DC. The Ministers discussed the work of the FATF in the international fight against money laundering and terrorist financing. They also endorsed a revised mandate for the FATF, which determines its direction and priorities between 2008 and 2012. (refer to the **FATF Revised Mandate 2008-2012**.)

Other international anti-money laundering initiatives include the following:

- **Asia/Pacific Group on Money Laundering** (APG);
- **Caribbean Financial Action Task Force on Money Laundering** (CFATF);
- **Egmont Group of Financial Intelligence Units**;\(^{66}\)
- **Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism** (May 16, 2005);
- **Organisation for Economic Co-operation and Development: Conventions on Combating Bribery of Foreign Public Officials in International Business Transactions**;
- **United Nations Convention against Corruption**;
- **United Nations Conventions on Terrorism**.

The United Nations **International Money Laundering Information Network** (IMoLIN) is an Internet-based network assisting governments, organizations and individuals in the fight against money laundering and the financing of terrorism. IMoLIN has been developed with the cooperation of the world’s leading anti-money laundering organizations. It includes a database on legislation and regulation throughout the world (including Canada), an electronic library and a calendar of events on anti-money laundering/countering the financing of terrorism.

---

\(^{65}\) Information on current FATF activities is available in FATF e-News and other online publications ([http://www.fatf-gafi.org/findDocument/0,3354,ea_32250379_32237245_1_32247548_1_1,00.html](http://www.fatf-gafi.org/findDocument/0,3354,ea_32250379_32237245_1_32247548_1_1,00.html)).

\(^{66}\) In February 2008, the Honourable Jim Flaherty, Canada’s Minister of Finance, officially opened the permanent headquarters of the secretariat of the Egmont Group in Toronto, Canada. The Egmont Group is an organization of 106 of the world’s financial intelligence units, including the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).
Australia

Australia is a member of the FATF. It was one of the first countries to enact legislation that: (1) made money laundering a criminal offence; (2) established a system to trace cash and, later, other forms of transfer of value; (3) provided a means to deal with the seizure and confiscation of proceeds of crime; and (4) allowed for mutual legal assistance with other countries. These measures were adopted in the *Proceeds of Crime Act 1987*, the *Financial Transaction Reports Act 1988* and the *Mutual Assistance in Criminal Matters Act 1987*.

According to *An Overview of Australia’s Anti-Money Laundering Strategy (May 2000)*, Australia continues to be a world leader due to its legislative framework, its analytical and law enforcement techniques, and its successful strategy of inter-agency cooperation. It has adopted a “whole system” approach to dealing with money laundering by putting in place appropriate law enforcement structures, legislation and operational techniques. Australia has taken the FATF philosophy and extended it to areas such as money laundering associated with tax evasion and cross-border reporting requirements to international wire transfers.

The Australian system gives high priority to the use of financial reports and related information for locating the money trail, particularly with regard to organized crime and serious criminal offenders. In this respect, the Australian Government has established the *Australian Transaction Reports Analysis Centre* (AUSTRAC), a specialized regulatory agency to work with the financial sector, to receive reports of significant and suspicious transactions and to analyze financial transaction data. That data in the form of intelligence is made available to Australia’s major law enforcement agencies and the Australian Taxation Office (ATO) to assist them in their actions against criminal activity and tax evasion.

A major feature of the Australian use of financial transaction data is the operation of a Task Force of agencies, including the Australian Bureau of Criminal Intelligence (which represents the States and Territories), the Australian Customs Service, the Australian Federal Police, the Australian Taxation Office, AUSTRAC and the National Crime Authority. This process ensures that information of importance is quickly and efficiently distributed to relevant law enforcement agencies. It has particular importance in the investigation of organized criminal activity but also assists in dealing with major tax avoidance and in uncovering practices that seek to defeat the reporting obligations of Australian law.

The FATF completed an assessment of the implementation of anti-money laundering and counter-terrorist financing standards in Australia in October 2005 (see *Mutual Evaluation of Australia*). Additional information and guidance is available online from the *Institute of Chartered Accountants in Australia*. 

United Kingdom

The United Kingdom (UK) is a member of the FATF and a sponsoring country of the CFATF. Overall, the UK anti-money laundering system meets the FATF 40 Recommendations. According to the FATF, many parts of the UK system provide a model that could be followed by other countries, with the system of education, training and Guidance Notes for the financial sector seeming to be particularly successful. The active system of supervision, cooperation, education and training in the financial sector are complemented by strong and effective penal legislation.

Several major pieces of penal legislation have been enacted, creating new money laundering offences and strengthening the confiscation legislation. The Money Laundering Regulations 1993 lay down requirements as to customer identification, record keeping, supervision and the reporting of suspicious transactions for a wide range of businesses. All firms of practicing accountants and some in business had to address new obligations in respect of money laundering when the Proceeds of Crime Act 2002 and the Money Laundering Regulation 2003 came fully into effect on March 1, 2004.

The Serious Organized Crime Agency (SOCA) has an important role in the UK’s anti-money laundering initiative. Active measures have also been taken with respect to international cooperation and many new bilateral confiscation agreements have been entered into. These measures have been complemented by administrative steps such as improving the Guidance Notes for financial institutions and the procedures relating to the reporting and investigation of suspicious transaction reports, improving feedback to financial institutions, and increasing the awareness of money laundering for non-financial businesses.

The FATF completed an assessment of the implementation of anti-money laundering and counter-terrorist financing standards in the United Kingdom in July 2007 (see Mutual Evaluation of the UK). Additional guidance is available online from the Institute of Chartered Accountants in England and Wales.
United States
The United States (US) is a member of the FATF and the Asia Pacific Group on Money Laundering, as well as a sponsoring country of the CFATF. Due in part to the size and sophistication of the United States financial system and the country’s geographical proximity to the drug producing countries of South America, the US continues to have a very serious money laundering problem. It is estimated that 60-80% of federal money laundering cases involve narcotics proceeds. Significant illegal proceeds are also generated by offences connected to organized crime and white-collar crime, where criminal groups are often formed along ethnic or national lines. In addition, there is considerable laundering of the proceeds from foreign crimes.

The US anti-money laundering system meets the FATF’s 40 Recommendations in most respects. Nonetheless, the system is not as effective or efficient as it could be because of the multitude of law enforcement and regulatory agencies, the large number of financial institutions, the diversity of federal and state laws, and the absence of comprehensive statistics to make informed resource allocation decisions.

In the US, money laundering is addressed in the provisions of the *Bank Secrecy Act* (BSA, Titles I and II of Public Law 91-508) and related regulations (31 CFR Part 103), the federal “Money Laundering Laws” (18 U.S.C. 1956–1960) and the rules and regulations issued by the federal bank supervisory agencies, the SEC and securities industry self-regulatory organizations and the US Department of the Treasury. These provisions govern most of the registration, record keeping, reporting and control obligations that financial institutions and individuals have with respect to money laundering. They also establish civil and criminal penalties for failure to meet related obligations.

The BSA (31 U.S.C. 5312(a)(2)) defines many kinds of businesses as “financial institutions.” Currently, banks and bank holding companies and their non-bank subsidiaries are required to report suspicious activity to the Treasury under federal regulations. Because this requirement also applies to financial institution employees, including certified public accountants (CPAs), practitioners need to be sure which entities are affected. In addition, many non-bank financial institutions that are not currently required to report suspicious activity are increasingly doing so on a voluntary basis, and the “safe harbor” provided by the BSA protects them and their employees against their customers’ civil claims. It is expected that mandatory reporting of suspicious activity will be extended to others within the financial services industry.

Since its creation in 1990 by the US Department of the Treasury, the [Financial Crimes Enforcement Network](http://www.fincen.gov) (FinCEN) has worked to support law enforcement investigative efforts and foster inter-agency and global cooperation against domestic and international financial crimes. It provides US policy makers with strategic analyses of domestic and worldwide trends and patterns. In addition, through information collection, analysis and sharing, as well as technological assistance, it provides cost-effective implementation of the BSA and other Treasury authorities.
In 1998, the *Money Laundering and Financial Crimes Strategy Act* chartered a joint Treasury and Justice Department initiative to develop a broad, comprehensive strategy to combat money laundering at federal, state and local levels. In this regard, a report entitled “The National Money Laundering Strategy for 2000,” contemplated methods accountants and auditors can use to help detect and deter money laundering. The “2001 National Money Laundering Strategy” recognizes that money laundering is an integral component of large-scale criminal enterprises. It notes that drug trafficking, firearms smuggling, international bank and securities frauds, bribery, intellectual property theft, and other specified unlawful activity generate illicit proceeds that criminals must conceal. It also warns of the negative roles lawyers, bankers and accountants can intentionally or unintentionally play in abetting criminal efforts to disguise unlawful income. It is noteworthy that most states now have some form of anti-money laundering or related asset seizure and forfeiture statute. These developments suggest that CPAs will be expected to contribute more to the fight against money laundering.

Following the terrorist attacks against the United States on September 11, 2001, it was recognized that the fight against money laundering is integral to the war against terrorism, and that effective anti-money laundering policies will save innocent lives. In October 2001, the *USA Patriot Act* was issued which, among other provisions, targets money laundering activities. The *Treasury Department* is issuing a series of rules for implementation of the Act. Specific initiatives are set out in the “2007 National Money Laundering Strategy.”

The Financial Action Task Force (FATF) completed an assessment of the implementation of anti-money laundering and counter-terrorist financing standards in the United States in June 2006 (see *Mutual Evaluation of the US*). Additional information and guidance is available online from the *Securities and Exchange Commission* (SEC). In addition, the United Nations *International Money Laundering Information Network* (IMoLIN) includes a database on legislation and regulation in the *United States*.

---


68 For more information, refer to the *Journal of Accountancy* articles: “The CPA’s Role in Fighting Money Laundering” by A.S. Abel and J.S. Gerson (June 2001); “Money Laundering: Ring Around The White Collar” by Joseph T. Wells (June 2003); and “Follow the Greenback Road” by Joseph T. Wells (November 2003).
New Zealand
New Zealand is a member of the FATF and the Asia Pacific Group on Money Laundering. Since 1994, New Zealand has significantly improved its compliance with the FATF 40 Recommendations with the introduction of a money laundering offence (amendment to the Crimes Act), the enactment of the Financial Transactions Reporting Act and the 1998 amendments to the Misuse of Drugs Act and the Mutual Assistance in Criminal Matters Act. These pieces of legislation provide a solid foundation for repressing, detecting and preventing money laundering in New Zealand.

The money laundering activity detected in New Zealand seems largely domestic in nature and is deemed by the authorities to be relatively small when considered in the international context. The main source of illegal proceeds can be categorized into three offences: drug; fraud and offences against property, including theft, burglary and receiving stolen goods. The offences generating the most money involve drugs followed by fraud and then other offences involving dishonesty. These offences tend to be the main focus of police efforts in identifying criminal proceeds.

The Ministry of Justice is currently reviewing and updating New Zealand’s anti-money laundering regime, aimed at countering the financing of terrorism and bringing New Zealand into line with international standards established by the FATF. New or amended legislation is expected to be enacted by the end of 2008. The United Nations International Money Laundering Information Network (IMoLIN) includes a database on legislation and regulation in New Zealand.

International Federation of Accountants (IFAC)
The International Federation of Accountants (IFAC) is urging the world’s accountants to participate in efforts to combat money laundering. In January 2002, IFAC published a paper on anti-money laundering aimed at promoting awareness of important money laundering issues and of the related professional obligations imposed on accountants. According to IFAC, the issue of money laundering has become even more important to regulators and law enforcement agencies around the world, particularly in their drive against the financing of terrorism.

In March 2004, IFAC published the second edition of the paper on Anti-Money Laundering. The paper discusses legislative and other measures taken to fight money laundering and the increased expectations that the profession monitor and detect money laundering, as well as establish and strengthen controls and safeguards against money laundering.
Appendix C

INDICATORS OF SUSPICIOUS TRANSACTIONS

This appendix lists common indicators that are set out in FINTRAC Guideline 2: Suspicious Transactions that might be useful in assessing whether a transaction is suspicious and should be reported.

The following indicators of suspicious transactions cover general matters, knowledge of money laundering reporting or record keeping requirements, identity documents, cash transactions, economic purpose, transactions involving accounts, transactions involving areas outside Canada, and transactions related to offshore business activity.

General

- Client admits or makes statements about involvement in criminal activities.
- Client does not want correspondence sent to home address.
- Client appears to have accounts with several financial institutions in one area for no apparent reason.
- Client conducts transactions at different physical locations in an apparent attempt to avoid detection.
- Client repeatedly uses an address but frequently changes the names involved.
- Client is accompanied and watched.
- Client shows uncommon curiosity about internal systems, controls and policies.
- Client has only vague knowledge of the amount of a deposit.
- Client presents confusing details about the transaction or knows few details about its purpose.
- Client appears to informally record large volume transactions, using unconventional bookkeeping methods or “off-the-record” books.
- Client over justifies or explains the transaction.
- Client is secretive and reluctant to meet in person.
- Client is nervous, not in keeping with the transaction.
- Client is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Client’s home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client shortly after opening account.
- Normal attempts to verify the background of a new or prospective client are difficult.
- Client appears to be acting on behalf of a third party, but does not tell you.
- Client is involved in activity out-of-keeping for that individual or business.
- Client insists that a transaction be done quickly.
- Inconsistencies appear in the client’s presentation of the transaction.
• The transaction does not appear to make sense or is out of keeping with usual or expected activity for the client.
• Client appears to have recently established a series of new relationships with different financial entities.
• Client attempts to develop close rapport with staff.
• Client uses aliases and a variety of similar but different addresses.
• Client spells his or her name differently from one transaction to another.
• Client uses a post office box or General Delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area.
• Client provides false information or information that you believe is unreliable.
• Client offers you money, gratuities or unusual favours for the provision of services that may appear unusual or suspicious.
• Client pays for services or products using financial instruments, such as money orders or traveller’s cheques, without relevant entries on the face of the instrument or with unusual symbols, stamps or notes.
• You are aware that a client is the subject of a money laundering or terrorist financing investigation.
• You are aware or you become aware, from a reliable source (that can include media or other open sources), that a client is suspected of being involved in illegal activity.
• A new or prospective client is known to you as having a questionable legal reputation or criminal background.
• Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).

Knowledge of Money Laundering Reporting or Record Keeping Requirements
• Client attempts to convince employee not to complete any documentation required for the transaction.
• Client makes inquiries that would indicate a desire to avoid reporting.
• Client has unusual knowledge of the law in relation to suspicious transaction reporting.
• Client seems very conversant with money laundering issues.
• Client is quick to volunteer that funds are “clean” or “not being laundered.”
• Client appears to be structuring amounts to avoid record keeping, client identification or reporting thresholds.
• Client appears to be collaborating with others to avoid record keeping, client identification or reporting thresholds.
• Client performs two or more cash transactions of less than $10,000 each just outside of 24 hours apart, seemingly to avoid the 24-hour rule.
Identity Documents

- Client provides doubtful or vague information.
- Client produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Client refuses to produce personal identification documents.
- Client only submits copies of personal identification documents.
- Client wants to establish identity using something other than his or her personal identification documents.
- Client’s supporting documentation lacks important details such as a phone number.
- Client inordinately delays presenting corporate documents.
- All identification presented is foreign or cannot be checked for some reason.
- All identification documents presented appear new or have recent issue dates.
- Client presents different identification documents at different times.
- Client alters the transaction after being asked for identity documents.
- Client presents different identification documents each time a transaction is conducted.

Cash Transactions

- Client starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the client in the past.
- Client frequently exchanges small bills for large ones.
- Client uses notes in denominations that are unusual for the client, when the norm in that business is much smaller or much larger denominations.
- Client presents notes that are packed or wrapped in a way that is uncommon for the client.
- Client deposits musty or extremely dirty bills.
- Client makes cash transactions of consistently rounded-off large amounts (e.g., $9,900, $8,500, etc.).
- Client consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Client consistently makes cash transactions that are significantly below the reporting threshold amount in an apparent attempt to avoid triggering the identification and reporting requirements.
- Client presents uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which could trigger reporting requirements.
- Client conducts a transaction for an amount that is unusual compared to amounts of past transactions.
- Client frequently purchases traveller’s cheques, foreign currency drafts or other negotiable instruments with cash when this appears to be outside of normal activity for the client.
- Client asks you to hold or transmit large sums of money or other assets when this type of activity is unusual for the client.
- Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc.)
• Stated occupation of the client is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).
• Cash is transported by a cash courier.
• Large transactions using a variety of denominations.

Economic Purpose
• Transaction seems to be inconsistent with the client’s apparent financial standing or usual pattern of activities.
• Transaction appears to be out of the ordinary course for industry practice or does not appear to be economically viable for the client.
• Transaction is unnecessarily complex for its stated purpose.
• Activity is inconsistent with what would be expected from declared business.
• A business client refuses to provide information to qualify for a business discount.
• No business explanation for size of transactions or cash volumes.
• Transactions of financial connections between businesses that are not usually connected (for example, a food importer dealing with an automobile parts exporter).
• Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

Transactions Involving Accounts
• Opening accounts when the client’s address is outside the local service area.
• Opening accounts in other people’s names.
• Opening accounts with names very close to other established business entities.
• Attempting to open or operating accounts under a false name.
• Account with a large number of small cash deposits and a small number of large cash withdrawals.
• Funds are being deposited into several accounts, consolidated into one and transferred outside the country.
• Client frequently uses many deposit locations outside of the home branch location.
• Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers.
• Activity far exceeds activity projected at the time of opening of the account.
• Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
• Account reactivated from inactive or dormant status suddenly sees significant activity.
• Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.
• Unexplained transfers between the client’s products and accounts.
• Large transfers from one account to other accounts that appear to be pooling money from different sources.
• Multiple deposits are made to a client’s account by third parties.
• Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.
• Frequent deposits of bearer instruments (for example, cheques, money orders or bearer bonds) in amounts just below $10,000.
• Unusually large cash deposits by a client with personal or business links to an area associated with drug trafficking.
• Regular return of cheques for insufficient funds.
• Correspondent accounts being used as “pass-through” points from foreign jurisdictions with subsequent outgoing funds to another foreign jurisdiction.
• Multiple personal and business accounts are used to collect and then funnel funds to a small number of foreign beneficiaries, particularly when they are in locations of concern, such as countries known or suspected to facilitate money laundering activities.

Transactions Involving Areas Outside Canada
• Client and other parties to the transaction have no apparent ties to Canada.
• Transaction crosses many international lines.
• Use of a credit card issued by a foreign bank that does not operate in Canada by a client that does not live and work in the country of issue.
• Cash volumes and international remittances in excess of average income for migrant worker clients.
• Excessive demand for migrant remittances from individuals or entities based on migrant worker population.
• Transactions involving high-volume international transfers to third party accounts in countries that are not usual remittance corridors.
• Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money laundering system.
• Transaction involves a country known for highly secretive banking and corporate law.
• Transactions involving countries deemed by the Financial Action Task Force as requiring enhanced surveillance, including the Republic of Nauru.
• Foreign currency exchanges that are associated with subsequent wire transfers to locations of concern, such as countries known or suspected to facilitate money laundering.
• Deposits followed within a short time by wire transfer of funds to or through locations of concern, such as countries known or suspected to facilitate money laundering activities.
• Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money-laundering system.
• Transaction involves a country known or suspected to facilitate money laundering activities.
Transactions Related to Offshore Business Activity

Any person or entity that conducts transactions internationally should consider the following indicators:

- Accumulation of large balances, inconsistent with the known turnover of the client’s business, and subsequent transfers to overseas account(s).
- Frequent requests for traveller’s cheques, foreign currency drafts or other negotiable instruments.
- Loans secured by obligations from offshore banks.
- Loans to or from offshore companies.
- Offers of multimillion-dollar deposits from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.
- Transactions involving an offshore “shell” bank whose name may be very similar to the name of a major legitimate institution.
- Unexplained electronic funds transfers by client on an in-and-out basis.
- Use of letter-of-credit and other method of trade financing to move money between countries when such trade is inconsistent with the client’s business.
- Use of a credit card issued by an offshore bank.
Appendix D

READINESS ASSESSMENT CHECKLIST FOR CAs and CA FIRMS

This Appendix provides a checklist to assist CAs and CA firms in meeting the requirements of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Not all questions will apply to all situations.

1. About Money Laundering (see Chapter 1, Appendix A and Appendix B)
   a) Do you understand the money laundering process?
   b) Are you (or your firm) subject to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) or other statutory provisions regarding money laundering (a legal interpretation may be required)?
   c) Do you have a strategic or business plan that addresses money laundering obligations?

2. Implementing a Compliance Program (see Chapter 2)
   a) Is senior management actively involved in the development, implementation and/or promotion of money laundering measures?
   b) Has a compliance officer or champion been designated?
   c) Have appropriate money laundering compliance policies and procedures been established with respect to:
      • assessing the risks related to money laundering and terrorist financing?
      • identifying reportable transactions?
      • completing and filing reports?
      • ascertaining identity and third party disclosure statements?
      • preparing, maintaining and retrieving required records?
      • handling a FINTRAC compliance audit search and seizure in the event one occurs?
   d) Is the effectiveness of the compliance system monitored and appropriate, timely remedial action taken?
   e) Has a training program been developed for all staff, including senior people, and for the ongoing training of new staff?
   f) Are changes and developments in the legislation, regulations and related guidelines regularly monitored?
   g) Are polices, procedures, manuals and staff training materials regularly updated?

3. Suspicious Transactions (see Chapter 3 and Appendix C)
   a) Do you understand what constitutes a “suspicious transaction”? If there are reasonable grounds to suspect that client transactions are related to a money laundering offence or a terrorist financing offence, the reporting requirements of the PCMLTFA apply.
   b) Have appropriate policies and procedures been established with respect to:
• identifying suspicious transactions?
• preparing and transmitting reports to FINTRAC?
• keeping records of suspicious transactions?

4. Prescribed Transactions (see Chapter 4)
   a) At any time, are cash transactions or electronic funds transfers of $10,000 or more completed on behalf of clients? If so, the reporting requirements of the PCMLTFA apply.
   b) Have appropriate policies and procedures been established with respect to:
      • preparing and transmitting reports to FINTRAC?
      • keeping records of large cash transactions?
      • ascertaining the identity of the person or entity involved in a large cash transaction?
      • taking measures to determine whether the person or entity is acting on behalf of a third party?
      • obtaining and retaining a third party disclosure statement?
   c) Is a receipt of funds record prepared for any amount of $3,000 or more, whether or not it is received in cash?

5. Cross-Border Currency and Monetary Instruments (see Chapter 5)
   a) At any time, are currency or monetary instruments of $10,000 or more transferred across the Canadian border on behalf of clients? If so, the reporting requirements of Part 2 of the PCMLTFA apply.
   b) Have appropriate policies and procedures been established with respect to:
      • preparing and transmitting reports to the CBSA?
      • examining and opening mail?
      • disclosing information obtained from opening mail?

6. Rules of Professional Conduct (see Chapter 6)
   a) Has a communications strategy been developed to fully disclose, in writing, the reporting obligations and other requirements under the PCMLTFA to any potential client, as well as existing clients on new and currently open engagements?
   b) Have appropriate policies and procedures been established with respect to:
      • client communications to ensure all new and existing clients understand the implications of this legislation?
      • protecting confidential client information?
      • knowingly or unknowingly becoming a party to a money laundering offence under the Criminal Code by failing to take appropriate action?

7. Implications for Practitioners involved in Audit, Review and Compilation Engagements (see Chapter 7)
   a) In the course of providing audit, review or compilation engagements, are appropriate steps taken to assess the risks of material misstatements arising from illegal activities?
   b) Have appropriate policies and procedures been established with respect to situations where money laundering and terrorist financing activities are encountered?
GLOSSARY

ACRONYMS

PCMLTFA – Proceeds of Crime (Money Laundering) and Terrorist Financing Act

CBSA – Canada Border Services Agency

CCMIR – cross-border currency and monetary instrument reporting

CRA – Canada Revenue Agency

CSIS – Canadian Security Intelligence Service

FATF – Financial Action Task Force on Money Laundering

FinCen – Financial Crimes Enforcement Network (US)

FINTRAC – Financial Transactions and Reports Analysis Centre of Canada


Guidelines – guidelines prepared by FINTRAC on the PCMLTFA and Regulations

IFAC – International Federation of Accountants

IMF – International Monetary Fund

LCTR – large cash transaction report

NCIS – National Criminal Intelligence Service (UK)

OECD – Organisation for Economic Co-operation and Development

OSFI – Office of the Superintendent of Financial Institutions

Regulations – Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations

STRR – Proceeds of Crime (Money Laundering) Suspicious Transaction Reporting Regulations

SWIFT – means the Society for Worldwide Interbank Financial Telecommunication.

UN – United Nations
MONEY LAUNDERING TERMS

**Accountant** – means a chartered accountant, a certified general accountant or a certified management accountant.

**Accounting firm** – means an entity that is engaged in the business of providing accounting services to the public and has at least one partner, employee or administrator that is an accountant.

**Act** – means the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* S.C., c. 17.

**Black-market peso exchange** – an underground network of currency brokers with offices in North America, the Caribbean and South America allows drug traffickers to exchange pesos for US dollars.

**Cash** – means coins referred to in section 7 of the *Currency Act*, notes issued by the Bank of Canada pursuant to the *Bank of Canada Act* that are intended for circulation in Canada or coins or bank notes of countries other than Canada.

**Centre** – means the Financial Transactions and Reports Analysis Centre of Canada established by section 41 of the *PCMLTFA*.

**Client** – means a person or an entity that engages in a financial transaction or activity with a person or an entity referred to in section 5 of the *PCMLTFA* and includes a person or an entity on whose behalf the person or entity that engages in the transaction or activity is acting.

**Electronic funds transfer** – means the transmission — through any electronic, magnetic or optical device, telephone instrument or computer — of instructions for the transfer of funds, other than the transfer of funds within Canada. In the case of SWIFT messages, only SWIFT MT 103 messages are included.

**Entity** – means a body corporate, a trust, a partnership, a fund or an unincorporated association or organization.

**Financial entity** – means an authorized foreign bank as defined in section 2 of the *Bank Act* in respect of its business in Canada or a bank to which that Act applies, a cooperative credit society, savings and credit union or caisse populaire that is regulated by a provincial Act, an association that is regulated by the *Cooperative Credit Associations Act*, a company to which the *Trust and Loan Companies Act* applies and a trust company or loan company regulated by a provincial Act. It includes a department or agent of Her Majesty in right of Canada or of a province when the department or agent is carrying out an activity referred to in section 45.

**Funds** – means cash, currency or securities or negotiable instruments or other financial instruments, in any form, that indicate a person’s or an entity’s title or interest in them.
Integration - the third of three recognized stages in the money laundering process that involves placing the laundered proceeds back in the economy to create the perception of legitimacy.

Layering - the second of three recognized stages in the money laundering process that involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds. This stage may also involve transactions such as the buying and selling of stocks, commodities or property.

Money laundering offence – means an offence under subsection 462.31(1) of the Criminal Code.

Monetary instruments – means the following instruments in bearer form or in such other form as title to them passes on delivery, namely,
(a) securities, including stocks, bonds, debentures and treasury bills; and
(b) negotiable instruments, including bank drafts, cheques, promissory notes, travellers’ cheques and money orders, other than warehouse receipts or bills of lading.
For greater certainty, this definition does not apply to securities or negotiable instruments that bear restrictive endorsements or a stamp for the purposes of clearing or are made payable to a named person and have not been endorsed.

Money services business – means a person or entity that is engaged in the business of remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network, or of issuing or redeeming money orders, traveller’s cheques or other similar negotiable instruments. It includes a financial entity when it carries out one of those activities with a person or entity that is not an account holder.

Nominees - family members, friends or associates who are trusted within the community, and who will not attract attention, are used to conduct by a money laundering transactions.

Person – means an individual.

Placement – the first of three recognized stages in the money laundering process that involves placing the proceeds of crime in the financial system.

Prescribed – means prescribed by regulations made by the Governor in Council.

Prescribed transaction – any transaction involving $10,000 or more in cash arising in the course of conducting certain activities on behalf of a client. Prescribed transactions include “cross-border currency and monetary instrument transactions” that involve the exporting or importing of $10,000 or more of cash or monetary instruments.

Structuring or “smurfing” - inconspicuous individuals, commonly referred to as “smurfs,” deposit cash or buy bank drafts at various institutions, or one individual carries out transactions for amounts less than the amount that must be reported to the government, and the cash is subsequently transferred to a central account.
Suspicious transaction – a transaction (whether attempted or completed) where, in the course of conducting certain activities on behalf of a client, there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence.

Terrorist activity – has the same meaning as subsection 83.01(1) of the Criminal Code.

Terrorist activity financing offence – means an offence under section 83.02, 83.03 or 83.04 of the Criminal Code, or an offence under section 83.12 of the Criminal Code arising out of a contravention of section 83.08 of that Act.
SELECTED BIBLIOGRAPHY

Canadian Money Laundering Legislation


Canadian Money Laundering Regulations


- *Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations* ([www.fintrac-canafe.gc.ca/reg/1-eng.asp](http://www.fintrac-canafe.gc.ca/reg/1-eng.asp))

Canadian Money Laundering Guidelines

- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) (www.fintrac.gc.ca/)
- FINTRAC office consolidation of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (www.fintrac-canafe.gc.ca/act-loi/ConsolA_30062007-eng.asp)
- FINTRAC office consolidation of the regulations to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (www.fintrac-canafe.gc.ca/reg/1-eng.asp)
  - 1 - Backgrounder
  - 2 - Suspicious Transactions
  - 3A - Submitting STR Reports to FINTRAC Electronically
  - 3B - Submitting STR Reports to FINTRAC by Paper
  - 4 - Implementation of a Compliance Regime
  - 5 - Submitting Terrorist Property Reports
  - 6 - Record Keeping and Client Identification
  - 7 – Submitting Large Cash Transaction Reports to FINTRAC
  - 8 – Submitting Electronic Funds Transfer Reports to FINTRAC
  - 9 – Alternative to Large Cash Transaction Reports to FINTRAC

Canadian Web Sites

- Canada Border Services Agency (CBSA) (www.cbsa-asfc.gc.ca/)
- Canada Revenue Agency (CRA) (www.cccra-adrc.gc.ca/)
- Canadian Security Intelligence Service (CSIS), (www.csis-scrs.gc.ca/)
- Department of Citizenship and Immigration – Canada (www.cic.gc.ca/)
- Department of Finance – Canada (www.fin.gc.ca/)
- Department of Justice – Canada (www.canada.justice.gc.ca/)
- Department of Public Safety – Canada (www.ps-sp.gc.ca/)
- Office of the Superintendent of Financial Institutions (OSFI) – Canada (www.osfi-bsif.gc.ca/)
- Royal Canadian Mounted Police (RCMP) (www.rcmp-grc.gc.ca)
International Web Sites

- Asia/Pacific Group on Money Laundering (APG) (www.apgml.org/)
- Australian Transactions and Reports Analysis Centre (AUSTRAC) (www.austrac.gov.au/)
- Caribbean Financial Action Task Force on Money Laundering (CFATF) (www.cfatf.org/)
- Egmont Group of Financial Intelligence Units (www.egmontgroup.org/)
- European Union
- Financial Action Task Force on Money Laundering (FATF) (www1.oecd.org/fatf/)
- Financial Crimes Enforcement Network (FinCEN) - United States Treasury Department (www.fincen.gov)
- International Federation of Accountants (IFAC) (www.ifac.org/)
- International Monetary Fund (www.imf.org/)
- Serious Organised Crime Agency - United Kingdom (www.soca.gov.uk/)
- Organisation for Economic Co-operation and Development (OECD) (www.oecd.org/)
- United Nations (UN)
  - International Money Laundering Information Network (www.imolin.org/imolin/index.html)
  - Conventions on Terrorism (http://untreaty.un.org/English/Terrorism.asp)