Compliance manual — PCMLTFA

TABLE OF CONTENTS

Purpose of manual

This *Compliance Manual* is a resource for CGAs and their firms to understand their obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and *Regulations* for implementing a compliance regime.

In preparing this manual, three assumptions have been made:

1. The CGA firm consists of two or more partners, one or more professional staff, and support staff performing administrative, secretarial, and reception duties.
2. The CGA firm expects to have a low volume of reportable transactions.
3. The responsible CGA for a transaction/client, under the supervision of the compliance officer, is primarily responsible for making decisions about reporting. Although the legislation requires both CGAs and their staff to report, it is clear that the responsible CGA on a matter is ultimately responsible, and likely subject to penalties, for any failure to comply.

This manual will have to be customized to suit your practice. Sole practitioners, for example, would serve as the compliance officer. Some firms may want to make the compliance officer responsible for both the decision-making and report-making functions. Other firms may prefer to have the responsible CGA perform the decision-making and report-making functions. This "decentralized" option might be more appropriate for larger firms because involving the compliance officer in all decisions to report might be impractical.

Materials used in preparing this manual

This manual is based in part on the legislation, regulations, and materials prepared by FINTRAC. The materials used include six of the following nine *Guidelines* prepared by FINTRAC:

Guideline 1: *Backgrounder*

Guideline 2: *Suspicious Transaction Reporting*

Guideline 3A: *Submitting Suspicious Transaction Reports to FINTRAC electronically*

Guideline 3B: *Submitting Suspicious Transaction Reports to FINTRAC by paper*

Guideline 4: *Implementation of a compliance Regime* — This *Guideline* describes in detail FINTRAC's expectations for an effective compliance regime.

Guideline 5: *Submitting Terrorist Property Reports to FINTRAC*

Guideline 6: *Record Keeping and Client Identification*

Guideline 7A: *Submitting Large Cash Transaction Reports to FINTRAC electronically*

Guideline 7B: *Submitting Large Cash Transaction Reports to FINTRAC by paper*

Other *Guidelines* by FINTRAC can be found at: http://www.fintrac.gc.ca.

Section 300 of the Public Practice Manual contains a detailed *PCMLTFA Guideline*, with reports, for compliance with the legislation. This *Compliance Manual*, section 500, forms part of that *PCMLTFA Guideline*. It is a requirement under the legislation for each person or entity covered under the legislation to have a compliance manual. Several parts of this manual need to contain information that is already present in Section 300. Where applicable, this manual will reference the appropriate subsection of the *PCMLTFA Guideline* rather than reproduce the information. When adapting this *Compliance Manual* for your own use, you must ensure that section 300 is included.

1. Introduction

1.1 Money laundering legislation

The *Proceeds of Crime (Money Laundering) Act* was passed in June 2000, and was amended in 2001 to become the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA). Since that time a number of amendments have come into force as of February 10, 2007, and June 30, 2007, with the vast majority of new requirements becoming effective June 23, 2008. The next critical date is December 30, 2008, at which time the *PCMLTF Administrative Monetary Penalties Regulations* will come into force.

The *Act* makes it mandatory for various individuals and entities, including accountants and accounting firms, to report a variety of transactions to a government agency called the *Financial Transactions and Reports Analysis Centre of Canada* (FINTRAC). The mandatory reporting is designed to assist in the detection and deterrence of money laundering and terrorist financing activities as well as to facilitate the investigation and prosecution of money laundering and terrorist financing offences.

1.2 Obligations of accountants and accounting firms

The *Act* imposes a burden on accountants and accounting firms, and creates a statutory requirement to act if you are involved in certain triggering activities. This obligation extends to agents of the firm or anyone else authorized to act on behalf of the firm. The requirements are extensive in scope and the penalties for non-compliance can be up to five years in jail, with fines up to $2,000,000. There are three provisions under which you might be obligated to act under the PCMLTFA. These are suspicious transaction reporting (STR), large cash transaction reporting (LCTR), and cross-border currency or monetary instruments reporting (CCMIR). The burden to report suspicious and large cash transactions is imposed only if the accountant acts in particular circumstances. In essence, the accountant must be participating in a transaction as either an *intermediary* or a *facilitator*. The cross-border reporting of currency or monetary instruments applies to all Canadians. It is important to understand your obligations under this legislation and to be familiar with this *Compliance Manual*.

1.3 Mandatory elements of the compliance regime

The *Regulations* require that individuals and entities required to report implement a formal compliance regime. The compliance regime must include, as far as practicable, the following five elements:

- A compliance officer
- A documented ongoing employee training program
- Written compliance policies and procedures
- An assessment and documentation of risks related to money laundering and terrorist financing
- A review of policies and procedures to test their effectiveness. The review must include a written report produced within 30 days after the review, detailing the findings, and any updates to your compliance policies and procedures, including the status of their implementation. If it has been determined that the risk is high for money laundering or terrorist financing, the report must also consider measures to mitigate this risk and a plan to take reasonable measures to keep client identification information up to date as well as conduct ongoing monitoring of financial transactions to detect suspicious transactions. The review must be completed at least once every two years.

This *Compliance Manual* sets out the internal policies and procedures that a firm has to adopt in order to comply with the legislative requirements. It is an integral part of an employee training program.

2. The compliance officer

2.1 Appointment of compliance officer

A confirmation memo of responsibility should be kept in the firm's compliance master file, such as:

[*Date*]

[*Firm name*]

[*Name of individual*] is appointed the compliance officer for this [*name of firm*]. He/she will report to the partners/shareholders at least quarterly on the progress of the compliance regime implementation as well as the review of policies and procedures and staff training. Any questions about the compliance regime must be directed to him/her. If the compliance officer is absent or not available, [*name of individual*] (alternate compliance officer) will assume the responsibilities of the compliance officer. If both individuals are absent or not available, any partner/shareholder can assume the role of and undertake the responsibilities of the compliance officer.

2.2 Role of the compliance officer

The compliance officer is responsible for the implementation of the compliance regime, including the development and implementation of this firm's compliance policies and procedures, periodically reviewing those policies and procedures, as well as training all professionals, staff, agents, or anyone else authorized to act on behalf of the firm.

He/she should be consulted on all transactions where the possibility of reporting may exist. This ensures all factors and available information are considered before the decision is made whether to file a report or not. If necessary, all other professionals, staff, agents, or anyone else authorized to act on behalf of the firm that might have information pertaining to the client or transaction should be consulted.

The compliance officer will maintain a **compliance file**. This file will be kept separately from any client file. It will contain all client-related information, worksheets, records, and any other documents relating to the particular transaction, and will document the reasons why the particular transaction was or was not reported.

All correspondence from FINTRAC, including confirmation receipts, must be given to the compliance officer to be maintained in the compliance file.

3. Employee training program

3.1 Who is to be trained?

All members of the CGA firm, professionals and staff, as well as agents or anyone else authorized to act on behalf of the firm, are required to have training so they can understand and comply with the obligations imposed on them by the legislation. They must become familiar with the firm's compliance policies and procedures. Because all professionals, staff, agents and other authorized persons will likely handle client information, the potential exists for all of them to become aware of suspicious transactions (including *attempted* suspicious transactions) in the course of performing their duties. They must know how to recognize suspicious or large cash transactions as well as cross-border currency or monetary instrument transactions. They need to know how each of these types of transactions is to be reported and under what circumstances.

3.2 Training objectives

The compliance officer should implement a training program for all professionals, staff, agents, and anyone else authorized to act on behalf of the firm. The objective of this training is to provide an overview of the legislation and how money laundering works, as well as the policies and procedures developed and described in this manual.

3.3 Training schedule

The compliance officer will schedule and conduct the training sessions. New professionals or staff who join the firm must receive training from the compliance officer before they begin to deal with clients. This training regime is required to be in written format, and must be ongoing.

The compliance officer should also schedule regular review/update training at least every two years to ensure that all professionals and staff continue to understand their obligations and are following the firm's policies and procedures. The compliance officer will also conduct further training sessions if there are any significant changes in the legislation.

4. Background to money laundering legislation

The legislation was designed to help detect and deter money laundering and terrorist financing activities, and to help investigations and prosecutions of money laundering and terrorist financing offences. The legislation implements reporting, record keeping, and client identification requirements for a number of different entities and professionals, including accountants and accounting firms, their staff, agents, and anyone else authorized to act on behalf of the accountant or accounting firm.

4.1 Who is covered by this Act?

The *Act* applies to the following:

- Deposit-taking institutions
- Life insurance companies, brokers and agents
- Securities dealers — including portfolio managers and investment counselors
- Foreign exchange dealers
- Money services businesses
- Accountants
- Real estate brokers or sales representatives
- Casinos
- Agents of the crown or provinces that sell money orders
- Employees of any of the above

Financial planners are covered under the Securities dealers section provided they are licensed to sell securities of any type (i.e., mutual funds, etc.). CGAs who possess other professional designations — such as a CFP *(Certified Financial Planner*) will be covered under the provisions of that section as well as the provisions relating to accountants.

4.2 What is money laundering?

Money laundering is defined as "any act or attempted act to disguise the source of money or assets derived from criminal activity." Essentially, it is the process where 'dirty money' is transformed into 'clean money.'

Under Canadian law, a money laundering offence involves concealing or converting property or the proceeds of property (e.g., money), knowing or believing that the property or proceeds were derived from the commission of another offence (known as a **predicate offence**).

Predicate offences are not limited to the drug-dealing offences commonly associated with money laundering. They also include:

- Bribery of judicial officers
- Child pornography
- Breach of trust by a public officer
- Forgery
- Keeping a common bawdy house
- Procuring juvenile prostitution
- Theft
- Extortion

- Frauds on the government
- Corrupting morals
- Keeping gaming or betting house
- Betting, pool-selling, and bookmaking
- Murder
- Robbery
- Secret commissions
- Fraudulent manipulation of stock exchange transactions
- Possessing and/or uttering counterfeit money
- Fraud

4.3 Stages of money laundering

The process of money laundering is ongoing. Dirty money is constantly being introduced into the system in an effort to clean it. There are three recognized stages in the money laundering cycle:

Placement stage **—** typically the first stage of the money laundering cycle, this involves the placing of the proceeds of crime ('dirty money') into the system.

Layering stage **—** typically the second stage of the cycle, although it also happens on a continuous basis even after the third stage has been completed. Layering involves executing layers of transactions to disguise the audit trail and the source of ownership. The money launderer also does this so that it will be more difficult to trace funds back to the original criminal activity that gave rise to the proceeds.

Integration stage **—** the third stage of the cycle is the placing of the laundered proceeds back into the economy to create a perception of legitimacy. This also involves the investment of these proceeds into otherwise legitimate business activities to earn additional so-called "legitimate" business profits on top of the criminal proceeds being earned by the owner of the funds.

4.4 Methods of money laundering

There are many known methods to launder money and, with advances in technology, more sophisticated ways are being devised every day. Some of the most common techniques are:

Nominees **—** use of family members, friends, or associates who are trusted within the community and who will not attract attention. This facilitates the concealment of the source and ownership of the funds involved.

Structuring (smurfing) **—** inconspicuous individuals obtain cash, buy bank drafts or money orders at various institutions, usually for amounts less than the thresholds for reporting. The drafts or money orders are usually made payable to other parties and, along with cash, are typically deposited to a central account.

Bulk cash asset purchases **—** individuals buy big-ticket items like cars, boats, and real estate for cash. Often these will be registered in other names to distance the launderer. The assets can then be sold and converted back to 'clean' cash.

Currency smuggling — funds are moved across borders to other countries to disguise the true source and ownership of the funds. They are typically taken to countries where there are few, if any, laws to record the ownership of funds entering the financial system. These countries tend to also be those with very strict bank secrecy laws. Methods for smuggling include mail, courier, and body packing.

Exchange transactions — proceeds of crime are used to buy foreign currency that can then be transferred to offshore bank accounts or converted back to functional currency at another institution.

Casino gambling — individuals bring cash into casino and buy casino chips/tokens. After gaming and placing a few small bets, they redeem the remainder of the chips/tokens and request a casino cheque (often made payable to another third party).

Black market peso exchange **—** this is a method primarily affecting the United States although Canada is not immune to it. There is an underground network of currency brokers who buy the US and Canadian dollars from the criminal and give them pesos. The brokers then sell for pesos these US and Canadian dollars to foreign companies, who use the funds to purchase goods in the US and Canada for sale back home.

4.5 What is a terrorist financing offence?

Under Canadian law, 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 crimes. This includes inviting someone else to provide property for this purpose. It also includes the use or possession of property to facilitate or carry out terrorist activities.

Terrorists need financial support to carry out terrorist activities and achieve their goals. In this respect, there is little difference between terrorists and other criminals in their use of the financial system. A successful terrorist group, much like a criminal organization, is one that is able to build and maintain an effective financial infrastructure. For this, it must develop sources of funding and means of obscuring the links between those sources and the activities the funds support. It needs to find a way to make sure that the funds are available and can be used to get whatever goods or services needed to commit terrorist acts.

The fundamental aim of terrorist financing is to obtain resources to support terrorist activities. The sums needed to mount terrorist attacks are not always large and the associated transactions are not necessarily complex.

4.6 Methods of terrorist financing

The methods used by terrorist groups to generate funds from illegal sources are often very similar to those used by "traditional" criminal organizations. 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 tracking terrorists' financial activities.

There are two primary sources of financing for terrorist activities. The first involves getting financial support from countries, organizations or individuals. The other involves revenue-generating activities.

Financial support

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. This could include, for example, donations to certain organizations that are known to have links to terrorists or terrorist groups.

Revenue-generating activities

The revenue-generating activities of terrorist groups may include criminal acts, and therefore may appear similar to other criminal organizations. Kidnapping and extortion can serve a dual purpose of providing needed financial resources while furthering the main terrorist objective of intimidating the target population. In addition, terrorist groups may use smuggling, fraud, theft, robbery, and narcotics trafficking to generate funds.

Financing for terrorist groups may also include legitimately earned income, which might include collection of membership dues and subscriptions, sale of publications, speaking tours, cultural and social events, as well as solicitation and appeals within the community. This fundraising might be in the name of organizations with charitable or relief status, so that donors are led to believe they are giving to a legitimate good cause. Worldwide, only a few non-profit organizations or supposedly charitable organizations have been implicated in terrorist financing networks in the past. In these cases, the organizations may in fact have carried out some of the charitable or relief work. Members or donors may have had no idea that a portion of funds raised by the charity was being diverted to terrorist activities. This type of "legitimately earned" financing might also include donations by terrorist group members of a portion of their personal earnings.

5. Compliance policies and procedures

5.1 Seven elements to compliance policies and procedures

In order to meet obligations under the legislation, compliance policies and procedures cover the following seven areas:

- Commencement dates for reporting
- Identification of reportable transactions
- Client identification and obtaining information
- Completion and filing of reports
- Record keeping
- Communication with clients
- Compliance reviews and search and seizure by FINTRAC or other authorities

5.2 Commencement dates for reporting

There are four reports that may have to be filed. The reports and their commencement dates are:

• Suspicious transaction report	November 8, 2001
• Large cash transaction report	January 31, 2003
• Terrorist property report	June 12, 2002
• Cross-border currency or monetary instruments report	January 6, 2003

5.3 Identification of reportable transactions

5.3.1 *Suspicious transactions*

Accountants or accounting firms are subject to the reporting of suspicious transactions when they engage in any of the following activities on behalf of any person or entity (other than your employer), or to give instructions in respect of those activities on behalf of any person or entity (other than your employer):

- the receipt or payment of funds,
- the purchase or sale of securities, real properties or business assets, or entities, or
- the transfer of any funds or securities by any means.

The *Act* states that, for greater certainty, it is not intended to apply to audits, reviews, or compilation engagements carried out in accordance with the recommendations set out in the *Handbook*.

When you report the transaction, you must also take reasonable measures before the transaction is reported to ascertain the identity of the individual who conducted the transaction. The only exceptions to this requirement are when you have either already identified the individual or if you believe that doing so will inform the individual that you are submitting an STR.

The compliance officer and the responsible partner/shareholder are responsible for determining whether a completed or attempted transaction is suspicious and must be reported. Therefore, if any professional, staff member, agent or anyone else authorized to act on behalf of the firm becomes aware of information that may indicate a transaction could be suspicious, that person must communicate that information to the compliance officer and/or the responsible partner/shareholder.

If the compliance officer is the responsible partner/shareholder for a particular transaction, the alternate compliance officer should be consulted in the decision-making process of whether to file a report or not.

It is important to note that there is no minimum dollar threshold for reporting suspicious transactions.

To identify a reportable suspicious transaction, four primary procedures have to be followed.

Procedure 1 **—** If you are a professional, staff member, agent, or anyone else authorized to act on behalf of the firm and you become aware of facts that indicate a transaction might be suspicious, you must report this to the responsible partner/shareholder immediately.

Procedure 2 **—** The responsible partner/shareholder and the compliance officer must determine whether you or the firm has been involved in one of the "triggering" activities.

If the answer to this question is **no**, meaning you or the firm has not been involved in a triggering activity, there is no obligation to report suspicious activity/transactions. The reasons why no report is filed should be documented and placed in the compliance file maintained by the compliance officer.

If the answer to this question is **yes**, meaning you or the firm has been involved in a triggering activity, then a potential reporting obligation arises and you must follow procedure 3.

Procedure 3 — The responsible partner/shareholder and the compliance officer must determine whether the transaction is suspicious of being related to a money laundering or terrorist financing offence. To assist you in making this decision, consult PPM Section 300, *Guideline on Money Laundering* and the FINTRAC *Guideline* 2: *Suspicious Transaction Reporting*.

If, in your judgement and the judgement of the compliance officer, the transaction is not suspicious, there is no obligation to file a report. The reasons for not filing the report should be documented and placed in the compliance file maintained by the compliance officer.

If, in your judgement and the judgement of the compliance officer, the transaction is suspicious of being related to a money laundering or terrorist financing offence, you must follow procedure 4.

Procedure 4 **—** If you must file a Suspicious transaction report (STR) see section **5.4 —** *Record keeping and client identification obligations* and section **5.5 —** *Completion and filing of reports* for procedures that have to be followed under these circumstances. A copy of the STR should be retained in the compliance file maintained by the compliance officer, along with a memorandum from the responsible partner/shareholder and compliance officer detailing the basis for their suspicion.

For illustrative examples for suspicious transaction reporting, see Exhibit 1: Determining obligation to report suspicious transactions, and Exhibit 2: Procedural process for reporting suspicious transactions.

Exhibit 1

Determining obligation to report suspicious transactions

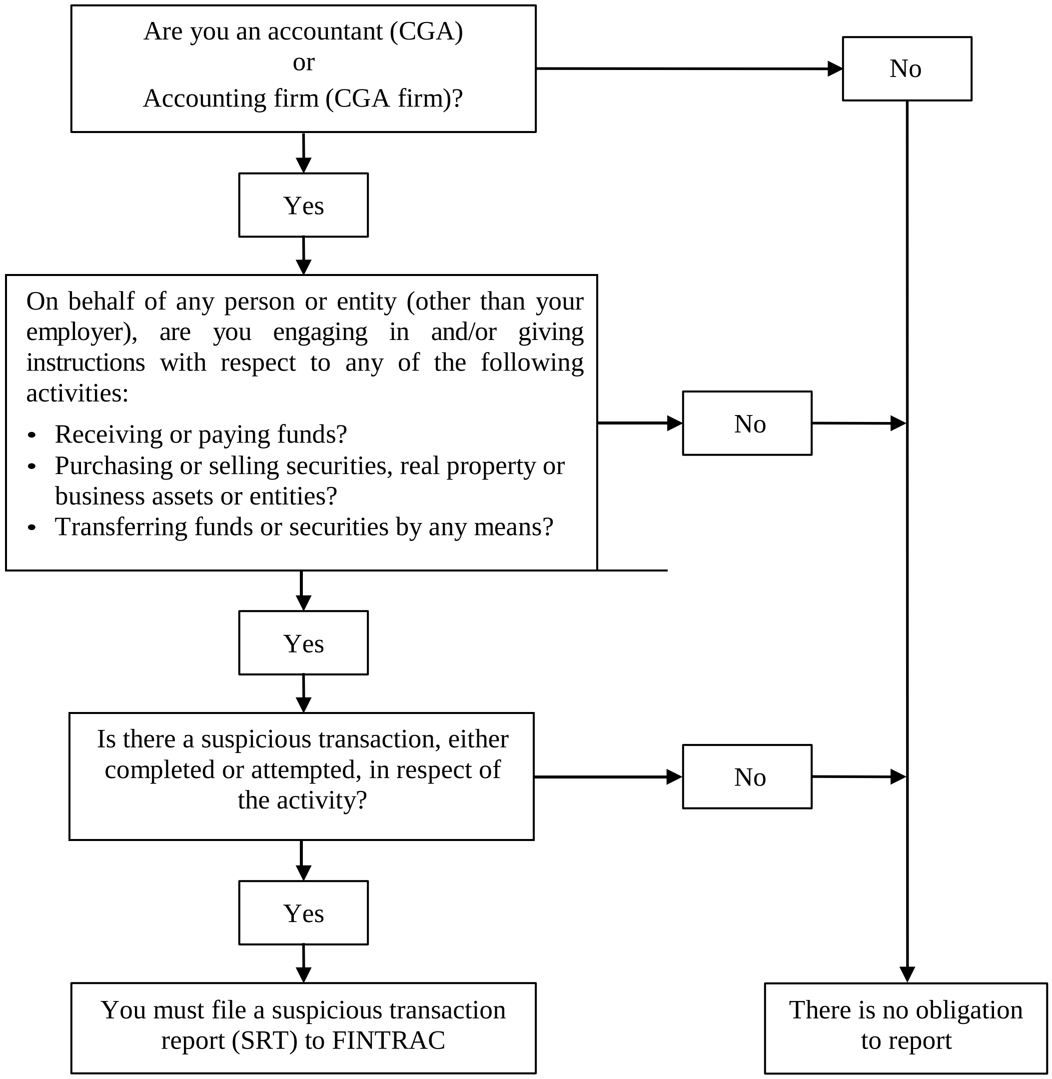
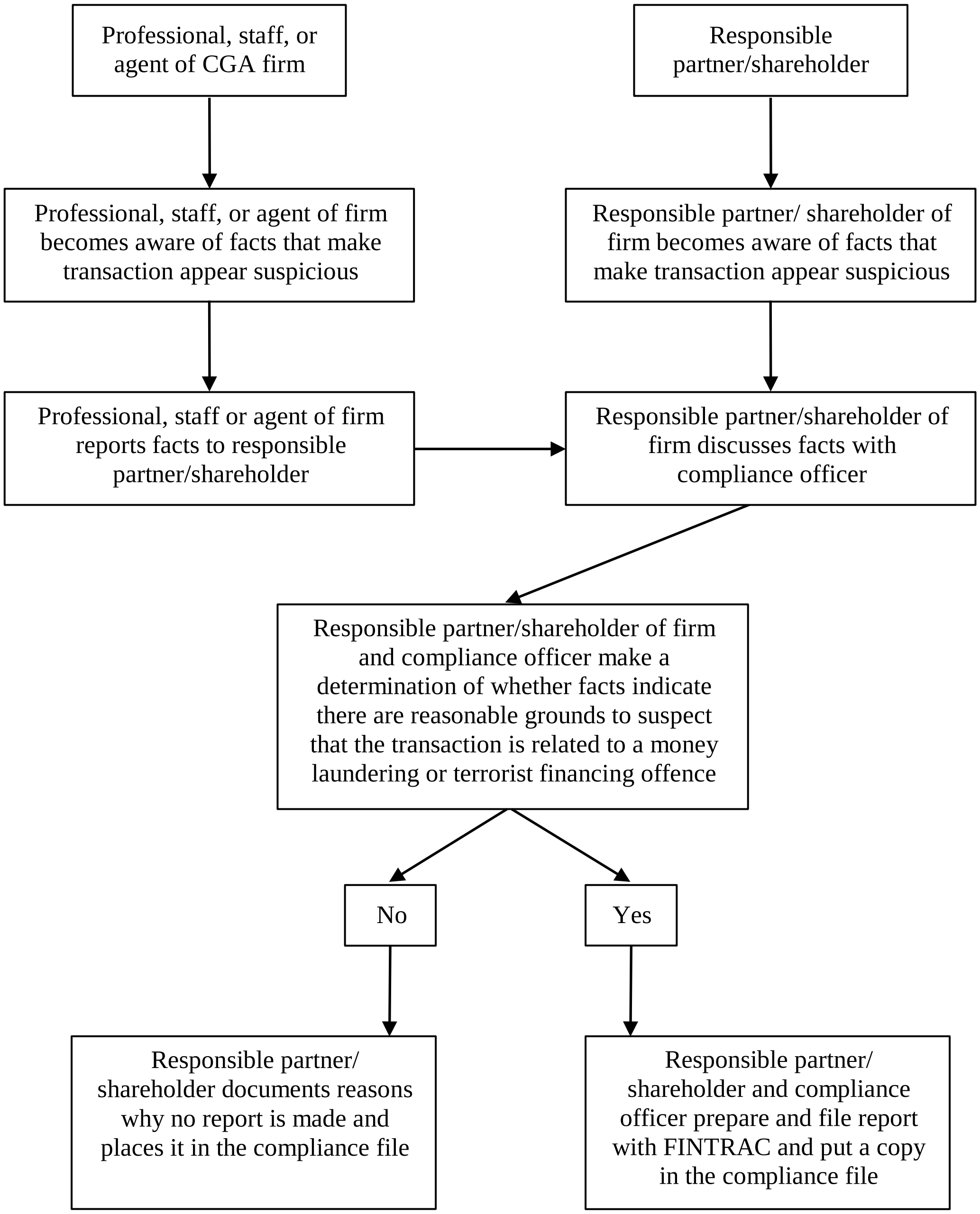


Exhibit 2

Procedural process for reporting suspicious transactions



5.3.2 *Large cash transactions*

Accountants or accounting firms are subject to the reporting of large cash transactions when they engage in any of the following activities on behalf of any person or entity (other than your employer), or give instructions in respect of those activities on behalf of any person or entity (other than your employer):

- the receipt or payment of funds,
- the purchase or sale of securities, real properties or business assets, or entities, or
- the transfer of any funds or securities by any means.

The *Act* states that, for greater certainty, it is not intended to apply to audits, reviews, or compilation engagements carried out in accordance with the recommendations set out in the *Handbook.*

To identify a reportable large cash transaction, six primary procedures have to be followed.

Procedure 1 — Determine whether you or the firm has been involved in one of the "triggering" activities.

If the answer to this question is **no**, meaning you or the firm has not been involved in a triggering activity, there is no obligation to report large cash transactions.

If the answer to this question is **yes**, meaning you or the firm has been involved in a triggering activity, then a potential reporting obligation arises and you must follow procedure 2.

Procedure 2 — Determine whether cash of $10,000 or more (in Canadian dollars or its equivalent) was received during the course of a single transaction. Remember that multiple payments within a 24-hour period that total more than $10,000 are to be considered a single transaction.

If cash of $10,000 or more was not received during the course of a single transaction, there is no obligation to report.

If cash of $10,000 or more was received during the course of a single transaction, a potential reporting obligation exists and you must follow procedure 3.

Procedure 3 — Determine whether the cash of $10,000 or more was received from a financial entity or public body.

If the cash of $10,000 or more was received from a financial entity or public body, there is no obligation to report.

If the cash of $10,000 or more was not received from a financial entity or public body, there is an obligation to report. See procedure 4 for additional requirements.

Procedure 4 — Take reasonable measures to determine whether the individual who in fact gives the cash is acting on behalf of a third party.

If they state that **they are not** acting on behalf of a third party and you **do not have** reasonable grounds to believe they actually are, you have no further obligations.

If they state that **they are not** acting on behalf of a third party and you **do have** reasonable grounds to believe they actually are, you must obtain a third-party disclosure statement.

If they state that **they are** acting on behalf of a third party, you must obtain a third-party disclosure statement.

***Procedure 5* —** Record and report the large cash transaction to FINTRAC. See section **5.4** — *Record keeping and client identification obligations* and section **5.5** — *Completion and filing of reports* for procedures that must be followed. The responsible partner/shareholder and the compliance officer will make a copy of any report filed and prepare a memorandum containing all the relevant information to be maintained in the compliance file.

***Procedure 6* —** The responsible partner/shareholder and the compliance officer should also review the context of the large cash transaction pursuant to the suspicious transaction procedures in **5.3.1** and determine whether a suspicious transaction report needs to be filed.

Definitions

Financial entity — is defined by FINTRAC as a bank, credit union, caisse populaire, a trust and loan company or an agent of the Crown or a Province that accepts deposit liabilities.

Public body — is defined by FINTRAC as any provincial or federal department or Crown agency, an incorporated municipal body (such as a city or town) and a hospital authority.

Third-party disclosure statements — Pursuant to the Regulations, when you determine that the individual conducting the transaction is acting on behalf of a third party, or there are reasonable grounds to believe this is the case, you must obtain and retain a third-party disclosure statement. The statement is to be signed by the individual conducting the transaction and it must include:

- If the third party is an individual, the individual's name, birthdate, address, and the nature of his/her principal business or occupation.
- If the third party is an entity, the entity's name, address, and the nature of its principal business. If the entity is a corporation, the corporation's incorporation number and its place of issuance.
- The nature of the relationship between the third party and the individual who is conducting the transaction.

If you are not able to determine whether the individual conducting the transaction is acting on behalf of a third party but there are reasonable grounds to suspect that they are, a record must be kept that includes:

- A statement from the individual conducting the transaction as to whether they are conducting it on behalf of a third party.
- A description of the reasons or reasonable grounds that cause you to suspect that the individual is in fact acting on behalf of a third party.

For an illustrative example for determining whether to report a large cash transaction see Exhibit 3: Determining obligation to report large cash transactions.

5.3.3 *Terrorist property — procedures under PCMLTFA*

Accountants or accounting firms are subject to the reporting of terrorist property when they engage in any of the following activities on behalf of any person or entity (other than your employer), or give instructions in respect of those activities on behalf of any person or entity (other than your employer):

- the receipt or payment of funds,
- the purchase or sale of securities, real properties or business assets, or entities, or
- the transfer of any funds or securities by any means.

The *Act* states that, for greater certainty, it is not intended to apply to audits, reviews, or compilation engagements carried out in accordance with the recommendations set out in the *Handbook*.

If you are a reporting person or entity, you have to submit a terrorist property report if you have property in your possession or control that you **know** is owned or controlled by or on behalf of a terrorist or a terrorist group. This includes information about any transaction or proposed transaction relating to that property.

To identify whether a terrorist property report must be made, three primary procedures have to be followed.

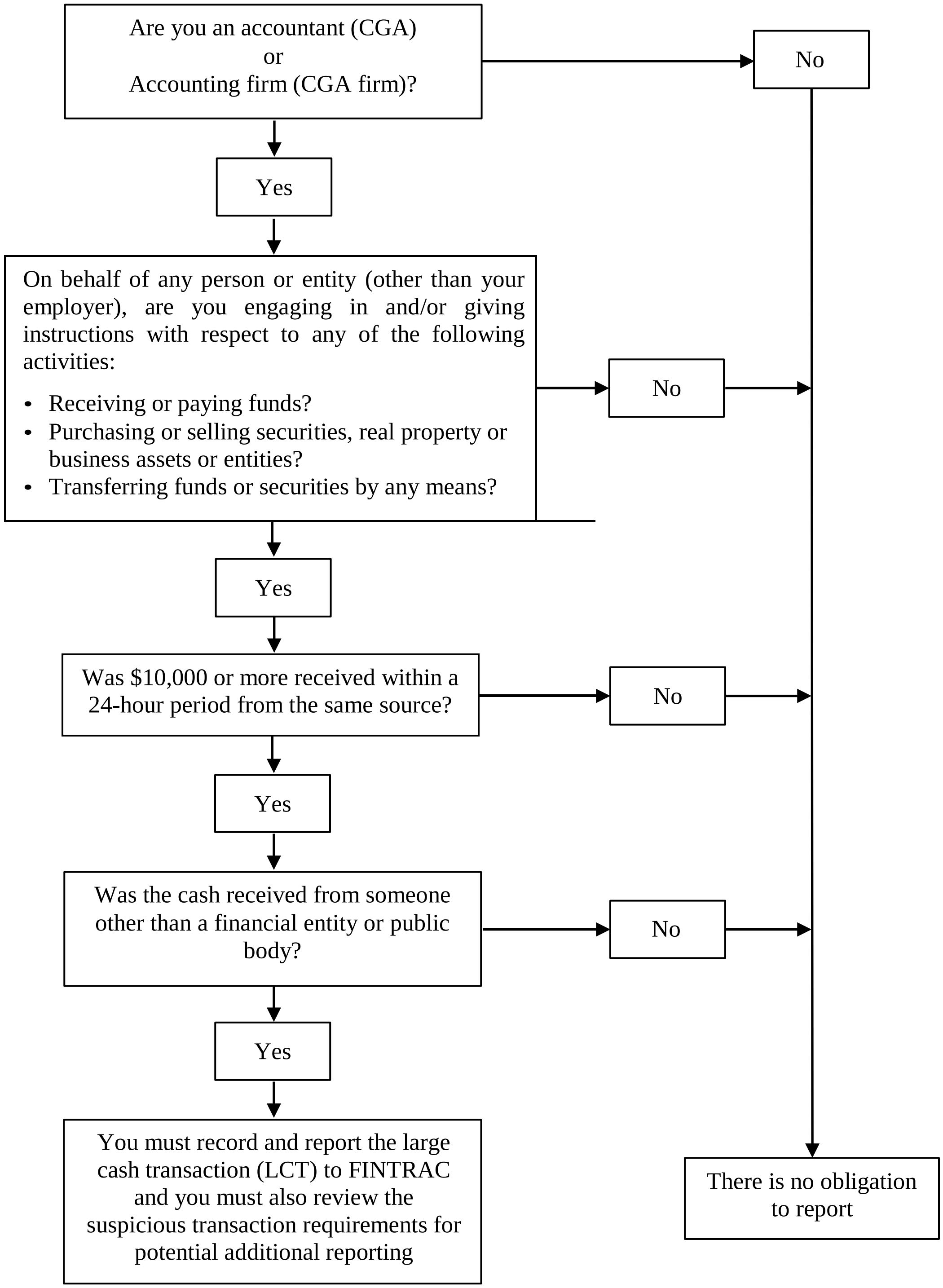
Procedure 1 — Determine whether you or the firm has been involved in one of the "triggering" activities.

If the answer to this question is **no**, meaning you or the firm has not been involved in a triggering activity, there is no obligation to report. However, see section **5.3.4** for potential reporting obligations under the Criminal Code.

If the answer to this question is **yes**, meaning you or the firm has been involved in a triggering activity, then a potential reporting obligation arises and you must follow procedure 2.

Exhibit 3

Determining obligation to report large cash transactions



Procedure 2 — Do you have property in your possession or control that you **know** is owned or controlled by or on behalf of a terrorist or a terrorist group?

If you **do not know** that the property in your possession or control is terrorist property and you **do not suspect** that it is, there is no obligation to report to FINTRAC. However, see section **5.3.4** for potential reporting obligations under the *Criminal Code*.

If you **do not know** that the property in your possession or control is terrorist property but **you suspect** that it is, there is no obligation to file a terrorist property report, but you may have to file a suspicious transaction report (STR) regarding such property. See section **5.3.1** for further instructions on this. Also, see section **5.3.4** for other potential reporting obligations.

If you have property in your possession or control that you **know** is owned or controlled by or on behalf of a terrorist or a terrorist group, including information about any transaction or proposed transaction relating to that property, you must file a terrorist property report to FINTRAC and see Procedure 3. Also, see section **5.3.4** for additional potential reporting obligations.

Procedure 3 — If you have property in your possession or control that you **know** is owned or controlled by or on behalf of a terrorist or a terrorist group, including information about any transaction or ***proposed transaction*** relating to that property, you may not complete or be involved in the proposed transaction. It is an offence under the *Criminal Code* to deal with any property if you know that it is owned or controlled by or on behalf of a terrorist or a terrorist group. It is also an offence to be involved in any transaction in respect of such property. In such circumstances, you are to remove yourself from any involvement and consult sections **5.3.3** and **5.3.4** regarding your reporting obligations.

Definitions

***Property* —** is defined by FINTRAC as any type of real or personal property. This includes, but is not limited to, any deed or instrument giving title or right to property, or any deed or instrument giving a right to money or goods. For example, cash, bank accounts, insurance policies, money orders, real estate, securities, and travelers cheques. This can also include business assets such as plant, property, and equipment.

For an illustrative example for determining whether to make a terrorist property report, see Exhibit 4: Determining obligation to report terrorist property.

5.3.4 *Terrorist property — procedures under the Criminal Code*

In addition to potentially making a terrorist property report to FINTRAC under the PCMLTFA (section **5.3.3**), the *Criminal Code* of Canada also has reporting requirements for terrorist property. These *Criminal Code* requirements apply to every person in Canada and any Canadian outside of Canada. It does not matter whether you are a reporting entity under the PCMLTFA or not and you do not have to be involved in any triggering activity before you are subject to the *Criminal Code* requirements.

The *Criminal Code* requires you to disclose to the RCMP and CSIS the existence of property in your possession or control that you **know** is owned or controlled by or on behalf of a terrorist or a terrorist group. This includes information about any transaction or proposed transaction relating to that property. Information is to be provided to the RCMP and CSIS, **immediately**, as follows:

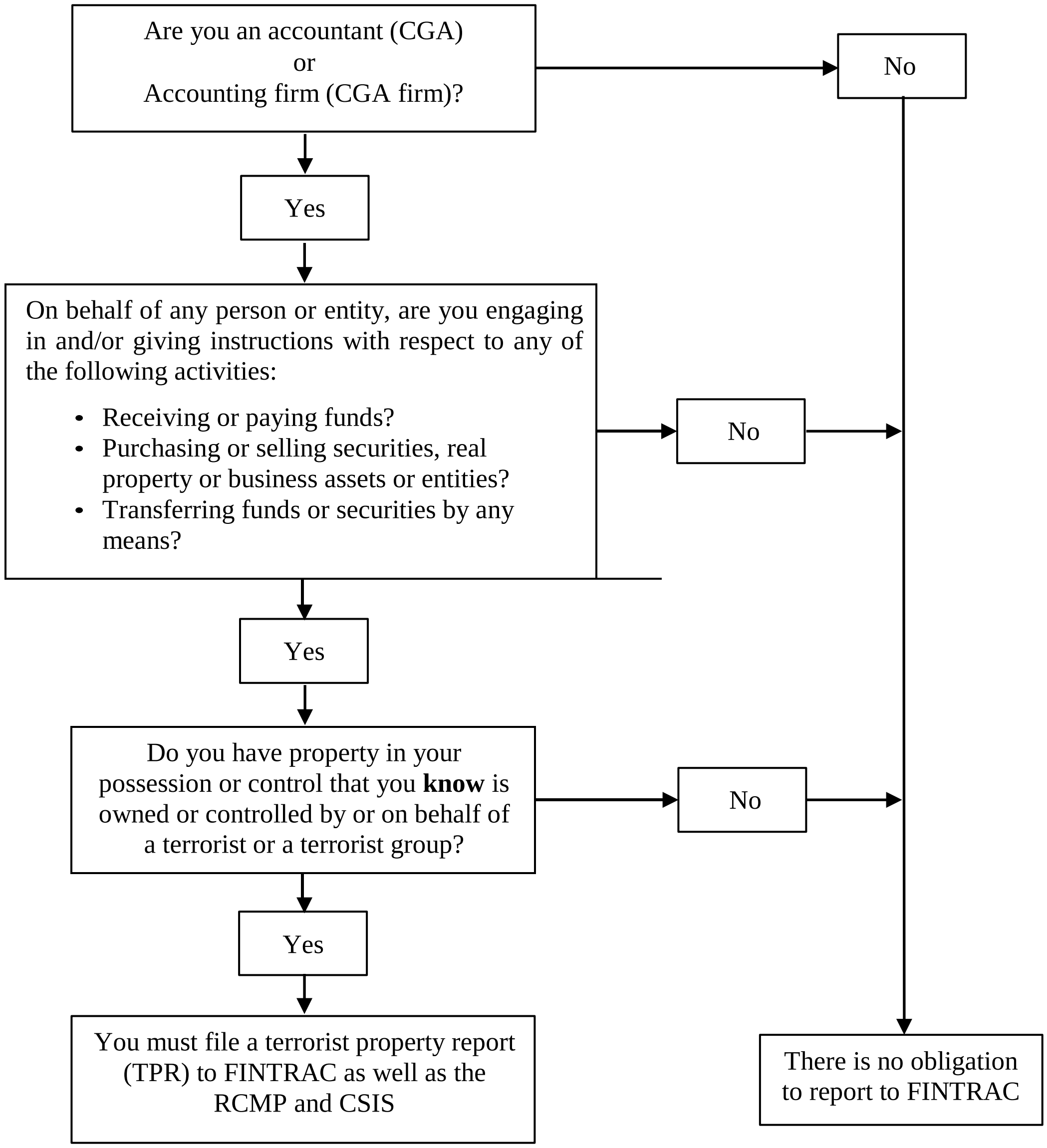
RCMP — Financial Intelligence Task Force unclassified fax: (613) 993-9474 or the RCMP Information Line: 1-888-349-9963

CSIS Security Screening Branch, Project Leader Government Operations, unclassified fax: (613) 842-1902

It is an offence under the *Criminal Code* to deal with any property if you know that it is owned or controlled by or on behalf of a terrorist or a terrorist group. It is also an offence to be involved in any transaction in respect of such property.

Exhibit 4

Determining obligation to report terrorist property



5.3.5 *Cross-border currency or monetary instruments (CCMIR)*

The *Act* requires every person in Canada to report every cross-border transfer of currency or monetary instruments that exceed $10,000 CND to the Canada Border Services Agency (CBSA).

Monetary instruments are defined as:

a) securities, including stocks, bonds, debentures, and treasury bills; and

b) negotiable instruments, including bank drafts, cheques, promissory notes, travelers cheques and money orders, other than

- warehouse receipts or bills of lading, and
- 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.

It does not matter whether you are a reporting entity under the PCMLTFA or not and you do not have to be involved in any triggering activity before you are subject to the requirements of the *Act*.

To identify whether a cross-border currency or monetary instruments report (CCMIR) must be made, three primary procedures have to be followed.

Procedure 1 — Determine whether you or the firm has imported or exported currency or monetary instruments across the border with a value greater than $10,000.

If the answer to this question is **no**, meaning you or the firm has not imported or exported currency or monetary instruments across the border with a value greater than $10,000 CND, there is no obligation to report.

If the answer to this question is **yes**, you must follow procedure 2.

Procedure 2 — Is the value of the currency or monetary instruments you or the firm has imported or exported across the border greater than $10,000.

If the answer to this question is **no**, there is no obligation to file a CCMIR. If the answer to this question is **yes**, you must see procedure 3.

Procedure 3 — If you answered **yes** to procedure 2 and the currency or monetary instruments were ***imported***, do any of the following ***exceptions*** to reporting apply:

- The currency or monetary instruments were in the actual possession of a person arriving in Canada, but Canada is only a transit point and they do not leave the airplane or customs area of the airport before departing for their final destination outside Canada.
- The currency or monetary instruments were imported by courier from a location outside Canada, but Canada is not the final destination and they are not removed from the secure customs area where they are temporarily held before departing for their final destination outside Canada.
- The currency or monetary instruments were mailed from a location outside Canada, but Canada is not the final destination and they are not removed from the course of post until after they have left Canada.

If the answer to this question is **yes**, meaning one of the exceptions applies, there is no obligation to file a CCMIR.

If the answer to this question is **no**, meaning none of the exceptions applies, you must file a CCMIR to the Canada Border Services Agency.

5.4 Record keeping and client identification obligations

Besides the various reporting obligations under the *Act*, accountants and accounting firms are subject to various record keeping and client identification obligations if they engage in or give instructions with respect to triggering activities.

5.4.1 *Large cash transaction record keeping and client identification*

When you conduct a large cash transaction, your record keeping and client identification obligations are:

- Keep a large cash transaction record;
- Identify the client; and
- Make a third-party determination and keep related records.

<u>Contents of a large cash transaction record</u>

The responsible partner/shareholder and the compliance officer should ensure that the following information is recorded in the LCTR and should sign each record made:

- The amount and currency of the cash received;
- The date and nature of the transaction;
- The purpose and details of the transaction;
- The type of transaction (for example, the cash was transferred to someone else, etc.);
- Whether any other individuals or entities were involved in the transaction;

- How the cash was received (for example, in person, by mail, etc.);
- The number and type of any account affected by the transaction (if applicable);
- The full name of the individual who holds the account or conducted the transaction;
- The individual's address and principal business or occupation;
- The individual's date of birth; the type of document used to confirm the individual's identity, the document's reference number and its place of issue;
- If the individual is acting on behalf of a third party (including his/her employer), include the third party's name, address, and principal business or occupation;
- The incorporation number and place of incorporation if the third party is a corporation; and
- The nature of the relationship between the third party and the individual who conducted the transaction.

The responsible partner/shareholder and compliance officer will ensure that only ***required*** information is provided in the report. The *CGA Canada Code of Ethical Principles and Rules of Conduct (CEPROC)* allows the practitioner to report client information that is ***required*** to be reported by Statute. Only information that is ***required*** may be reported without breaching the CEPROC; ***no voluntary information is to be included in the report***.

The record should be maintained in paper format so that it can be readily produced if requested by FINTRAC. The record can be kept in electronic format provided that a paper copy can be readily produced if requested by FINTRAC and also provided that an electronic signature of the individual who must sign the report is retained.

The compliance officer will ensure that the large cash transaction records are maintained for a period of at least five years following the date each record was created.

Obtaining client identification information

Information should be obtained according to the following procedures:

Procedure 1 — Identification will be obtained for all new clients at the start of the client relationship.

Procedure 2 — Copies of relevant client identification will be maintained in a permanent file for the client.

***Procedure 3* —** Types of original identification that will be acceptable are:

If the potential client is an individual, you will obtain and make a copy of:

- Birth certificate,
- Driver's licence,
- Passport, or
- Other similar record issued by the provincial, territorial, or the federal government.

You may use the individual's provincial health card, provided there is no provincial or territorial legislation preventing you from requesting or using it. For example, Ontario, Manitoba, and Prince Edward Island prohibit health cards from being used for this purpose.

If the potential client is a corporation, you will need to obtain and make a copy of:

- Certificate of status,
- Articles of incorporation, and
- Provincial annual returns.

If the potential client is any other type of entity besides an individual or corporation, you need to obtain and make a copy of:

- Partnership agreement,
- Articles of association,
- Trust indenture, and
- Other similar record that proves existence.

If the potential client is unable to produce any of the listed identification, it is advisable not to accept them as a client.

Individual not physically present

If the transaction involves an individual who is not physically present, you can use an agent to verify identification on your behalf. However, unless you use an agent or mandatary, you are able to use a combination of *two* of the following methods to confirm the identity of an individual who is not present:

- Referring to an independent identification product or, with the individual's permission, referring to a credit file;
- Obtaining an attestation concerning an identification document for the individual from a commissioner of oaths or a guarantor;
- Confirming that a cheque drawn on a deposit account with a financial institution (other than one which is exempt from identification requirements) has cleared; and
- Confirming that the individual has a deposit account with a financial institution (other than one which is exempt from identification requirements).

For the purpose of satisfying the confirmation of identity in two different methods, you may not combine two of the sources in the first bullet, nor can you combine the method suggested in the second and third bullets.

You should rely on a combination of these methods only if the individual's information obtained is consistent within each method and with the information you have contained in your records.

Use of an agent or mandatary

If you rely on agents or mandataries to identify any of your clients, you must enter into a written agreement with them to do so. You must also obtain from the agent or mandatary the customer information that was obtained according to the agreement.

This will only be acceptable when the agent or mandatary identifies the individual using an original identification document.

When you have to identify an entity on whose behalf a transaction is conducted, you will have to do so within 30 days after the transaction. When you have to identify an individual who conducts a transaction, you have to do so at the time of the transaction.

Third-party determination and related records

Please refer to 5.3.2 for requirements for third-party determination and record keeping.

5.4.2 *Suspicious transaction report records and obtaining client identification*

When you are required to submit a suspicious transaction report to FINTRAC, you must take reasonable measures, before the transaction is reported, to identify the client who conducted it, unless the following circumstances exist:

- You had already identified the client as required and you have no doubts about that previous identification information; or
- You believe that doing so would inform the client that you are submitting a suspicious transaction report.

Please refer to 5.4.1 for the procedures for obtaining client identification information and identifying an individual not physically present.

You are required to keep a copy of the suspicious transaction report.

5.4.3 *Receipt of funds records and obtaining client identification*

When you receive funds in any form for an amount of $3,000 or more, your record keeping and client identification obligations are to:

- Keep a receipt of funds record; and
- Identify the client from whom the funds are received.

Content of a receipt of fund record

The content of a receipt of funds record is essentially the same as that of a large cash transaction (LCT) record. Please refer to section 5.4.1 for the content description, The received fund doesn't have to be cash, but if it is cash, you need to record how the cash was received, the same as is in a LCT record.

Obtaining client identification

Please refer to 5.4.1 for procedures for obtaining client identification information and identifying individuals not physically present.

Exceptions to receipt of funds records

If you have to keep a large cash transaction record, you do **not** have to keep a receipt of funds record for the same transaction. Also, you do **not** have to keep a receipt of funds record if the funds are received from a financial entity or a public body.

5.5 Completion and filing of reports

The *Act* stipulates that all suspicious transaction reports and large cash transaction reports must be filed electronically if you have the technical capabilities to do so. The minimum technical capabilities are:

- A personal computer with:
  - 32 MB memory
  - 640 × 480 VGA video display (800 × 600 or higher is preferable)
  - Any operating system running the following Web browsers: Internet Explorer version 5.x (Windows® 98/Me/NT/2000); and
- An internet connection

The *Act* also stipulates that there are three options for electronic reporting:

- FINTRAC's secure website for low-volume and low-frequency reporting;
- FINTRAC's secure website with public key infrastructure (PKI) for low-volume but high-frequency reporting; and
- Batch file transfer for high-volume and high-frequency reporting.

However, the *Act* does state that if the reporting person does not have the technical capabilities to file electronically, he or she can file by paper.

As the CGA firm has the technical capabilities to file electronically and anticipates a low volume and low frequency of reporting, all suspicious transaction reports and large cash transaction reports are to be submitted electronically via FINTRAC's secure website pursuant to the following procedures.

5.5.1 *Filing a suspicious transaction report (STR)*

If the responsible partner/shareholder and the compliance officer determine that an STR must be filed pursuant to the procedures contained in section 5.3.1, the subsequent procedures are to be followed:

Procedure 1 — Responsible partner/shareholder and the compliance officer will access FINTRAC's website at http://www.fintrac.gc.ca. Using the memorandum that documented the basis for their suspicion, they will undertake to complete the STR. (See Section 520 for directions on what information should be contained in the suspicious transaction report.)

Procedure 2 — Responsible partner/shareholder and compliance officer will ensure the report is filed within 30 days of the date on which reasonable grounds to suspect that the transaction is related to a money laundering or terrorist financing offence occurs. If suspicion occurs at the time of the transaction, the 30-day reporting timeline begins at the time of the transaction. If the suspicion occurs after the transaction or after multiple transactions, the 30-day reporting timeline begins at that later time.

Procedure 3 — Responsible partner/shareholder and compliance officer will ensure that only ***required*** information is provided in the report. The *CGA Canada Code of Ethical Principles and Rules of Conduct (CEPROC)* allows the practitioner to report client information that is ***required*** to be reported by Statute. Only information that is ***required*** may be reported without breaching the CEPROC; ***no voluntary information is to be included in the report***.

Procedure 4 — Responsible partner/shareholder and compliance officer will ensure all information required is provided and that reasonable efforts will be made to obtain any information that is required but not available at the time the report is being completed. The obligation to report is not fulfilled until a complete report is sent to FINTRAC.

Procedure 5 — Responsible partner/shareholder and the compliance officer will print off a hard copy of each page of the report.

Procedure 6 — Responsible partner/shareholder and compliance officer will ensure that the hard copy of the completed report, along with all supporting documentation and the memorandum they completed, are put into the compliance file.

Procedure 7 — When filing electronically, FINTRAC will send back an acknowledgement message that the report has been received. This acknowledgement will include the date and time the report was received and a FINTRAC-generated identification number. The responsible partner/shareholder and the compliance officer will ensure this acknowledgement message is filed in the compliance file.

Procedure 8 — If the STR contains incomplete information, FINTRAC may notify the firm. The notification will indicate the date and time the report was received, and a FINTRAC-generated identification number, along with information on the fields that must be completed or corrected. The responsible partner/shareholder and the compliance officer will ensure that such requests are responded to within the initial 30-day reporting time period. A copy of any such notice, as well as the additional information submitted to FINTRAC, will be placed in the compliance file along with all other documentation relating to this report.

5.5.2 *Filing a large cash transaction report (LCTR)*

If the responsible partner/shareholder and the compliance officer determine that a LCTR must be filed pursuant to the procedures contained in section 5.3.2, the subsequent procedures are to be followed:

Procedure 1 — Responsible partner/shareholder and the compliance officer will access FINTRAC's website at http://www.fintrac.gc.ca and complete the LCTR. (See Section 530 for directions on what information should be contained in the large cash transaction report.)

Procedure 2 — Responsible partner/shareholder and compliance officer will ensure the report is filed within 15 days after the transaction.

Procedure 3 — Responsible partner/shareholder and compliance officer will ensure that only ***required*** information is provided in the report. The *CGA Canada Code of Ethical Principles and Rules of Conduct (CEPROC)* allows the practitioner to report client information that is ***required*** to be reported by Statute. Only information that is ***required*** may be reported without breaching the CEPROC; ***no voluntary information is to be included in the report***.

Procedure 4 — Responsible partner/shareholder and compliance officer will ensure all information required is provided and that reasonable efforts will be made to obtain any information that is required but not available at the time the report is being completed. The obligation to report is not fulfilled until a complete report is sent to FINTRAC.

Procedure 5 — Responsible partner/shareholder and compliance officer will ensure that a third-party disclosure statement has been obtained if required. If it is, the responsible partner/shareholder and/or the compliance officer will obtain such third-party disclosure statement from the individual conducting the transaction.

Procedure 6 — Responsible partner/shareholder and compliance officer will ensure that the hard copy of the completed report, along with all supporting documentation and the memorandum they completed, are put into the compliance file. (*See section 5.6 — Record Keeping for additional details*)

Procedure 7 — When filing electronically, FINTRAC will send back an acknowledgement message that the report has been received. This acknowledgement will include the date and time the report was received and a FINTRAC-generated identification number. The responsible partner/shareholder and the compliance officer will ensure this acknowledgement message is filed in the compliance file.

Procedure 8 — If the LCTR contains incomplete information, FINTRAC may notify the firm. The notification will indicate the date and time the report was received, and a FINTRAC-generated identification number, along with information on the fields that must be completed or corrected. The responsible partner/shareholder and the compliance officer will ensure that such requests are responded to within the initial 15-day reporting time period. A copy of any such notice, as well as the additional information submitted to FINTRAC, will be placed in the compliance file along with all other documentation relating to this report.

5.5.3 *Filing a terrorist property report (TPR)*

At the present time, a terrorist property report can only be paper filed.

If the responsible partner/shareholder and the compliance officer determine that a TPR must be filed pursuant to the procedures contained in section 5.3.3, the subsequent procedures are to be followed:

Procedure 1 — Responsible partner/shareholder and the compliance officer will access FINTRAC's website at http://www.fintrac.gc.ca. They will print off the TPR file. (See Section 540 for directions on what information should be contained in the terrorist property report.)

Procedure 2 — Responsible partner/shareholder and compliance officer will ensure the report is filed **immediately** once it is determined that they are in possession or control of property that is owned or controlled by or on behalf of a terrorist or terrorist group.

Procedure 3 — Responsible partner/shareholder and compliance officer will ensure that only ***required*** information is provided in the report. The *CGA Canada Code of Ethical Principles and Rules of Conduct (CEPROC)* allows the practitioner to report client information that is ***required*** to be reported by Statute. Only information that is ***required*** may be reported without breaching the CEPROC; ***no voluntary information is to be included in the report***.

Procedure 4 — Responsible partner/shareholder and compliance officer will ensure all information required is provided and that reasonable efforts will be made to obtain any information that is required but not available at the time the report is being completed. The obligation to report is not fulfilled until they send a complete report to FINTRAC.

Procedure 5 — Responsible partner/shareholder and the compliance officer will then fax a copy of the report to the following:

- FINTRAC at (866) 226-2346
- RCMP, Financial Intelligence Task Force unclassified fax at (613) 993-9474
- CSIS, Security Screening Branch, Project Leader Government Operations, unclassified fax (613)842-1902.

If the responsible partner/shareholder and the compliance officer determine that the firm has not been involved in one of the triggering activities described in section 5.3.3, then the report will only be faxed to the RCMP and CSIS pursuant to the relevant sections of the *Criminal Code*. Since the *Criminal Code* is also a statute, disclosure under these circumstances will be covered by the exclusion contained in the CEPROC.

Procedure 6 — Responsible partner/shareholder and the compliance officer will ensure a copy of the completed report along with all supporting documentation and the memorandum they completed are put into the compliance file.

5.5.4 *Filing a cross-border currency or monetary instruments report (CCMIR)*

At the present time, CCMIRs can only be paper filed.

If the responsible partner/shareholder and the compliance officer determine that a CCMIR must be filed pursuant to the procedures contained in section 5.3.3, the subsequent procedures are to be followed:

Procedure 1 — Responsible partner/shareholder and the compliance officer will complete the report in the approved format. (See Section 550 for directions on the format and what information should be contained in the CCMIR.)

Procedure 2 — Responsible partner/shareholder and compliance officer will ensure the report is filed when due. The due date and place of delivery will depend on whether the currency or monetary instruments are imported or exported.

Procedure 3 — If the currency or monetary instruments are imported, the responsible partner/shareholder or the compliance officer will ensure that:

a) If the currency or monetary instruments are carried in person, the report is made to the Customs office at the point of entry into Canada.

b) If the currency or monetary instruments are carried by courier, the responsible partner/shareholder or the compliance officer will ensure that the exporter of the currency or monetary instruments has provided the necessary report to the courier for presentation to the Customs office where the package enters Canada.

c) If the currency or monetary instruments are imported by mail, the responsible partner/shareholder or the compliance officer will ensure the exporter of the currency or monetary instruments attaches the necessary report inside the mail being delivered and that the appropriate Customs Declaration form is attached to the outside of the envelope identifying that it contains currency or monetary instruments.

d) If the currency or monetary instruments are imported by courier or mail and the exporter does not provide the necessary report required, the responsible partner/shareholder will ensure that the necessary report is filed with Canada Border Services Agency immediately upon receipt of the courier or mail package. This report will be filed at the nearest CBSA office.

If the currency or monetary instruments are exported rather than imported, see Procedure 4.

Procedure 4 — If the currency or monetary instruments are exported, the responsible partner/shareholder or compliance officer will ensure that:

a) If the currency or monetary instruments are carried in person, the report is made to the Customs office at the point of exit from Canada.

b) If the currency or monetary instruments are exported by courier, the responsible partner/shareholder or the compliance officer will ensure that the courier company has the necessary report for presentation by the courier company to the Customs office at the point of exit from Canada.

c) If the currency or monetary instruments are exported by mail, the responsible partner/shareholder or the compliance officer will ensure the necessary report is included inside the envelope or package. The responsible partner/shareholder or compliance officer will also ensure that a copy of the report is mailed or submitted, at or before the time of mailing, to the Customs office that is located nearest to the point at which the item was or will be mailed.

Procedure 5 — Responsible partner/shareholder and compliance officer will ensure only ***required*** information is provided in the report. The CGA *Canada Code of Ethical Principles and Rules of Conduct (CEPROC)* allows the practitioner to report client information that is

required to be reported by Statute. Only information that is ***required*** may be reported without breaching the CEPROC; ***no voluntary information is to be included in the report***.

Procedure 6 — Responsible partner/shareholder and compliance officer will ensure all information required is provided and that reasonable efforts will be made to obtain any information that is required but not available at the time the report is being completed. The obligation to report is not fulfilled until a complete report is sent to CBSA.

Procedure 7 — Responsible partner/shareholder and the compliance officer will ensure a copy of the completed report, along with all supporting documentation and the memorandum they completed, are put into the compliance file.

5.6 Compliance file

Section 5.4 describes the record keeping and client identification obligations under the *Act* and related regulations. However, it may be prudent that additional records be kept and maintained in a compliance file, even though they are not required by the *Act* and related regulations. The compliance officer will maintain a compliance file, which contains all client-related information, worksheets, records, and any other documents relating to the particular transaction, as well as a description of reasons why the particular transaction was or was not reported.

The compliance file should be kept separately from any client file and should be in the possession and control of the compliance officer. The following procedures will outline the types of records that have to be kept, the format they have to be kept in, and the time period for retention of the records.

Procedure 1 — The compliance officer should ensure that the compliance file is maintained separately and apart from all client files.

Procedure 2 — The compliance officer should ensure that the following information is contained in the compliance file:

- Documentation and memorandums for all transactions considered under the suspicious transaction guidelines but determined not to be reportable, including the reasons why the transaction was not reported;
- Documentation, memorandums, and copies of the report filed for all suspicious transaction reports filed with FINTRAC;
- Acknowledgements and requests for additional information for all suspicious transaction reports filed with FINTRAC;
- Documentation and memorandums for all transactions considered to be large cash transactions but determined not to be reportable, including the reasons why the transaction was not reported;
- Documentation, memorandums, and copies of the report filed for all large cash transaction reports filed with FINTRAC;
- Acknowledgements and requests for additional information for all large cash transaction reports filed with FINTRAC;
- Documentation for all transactions and property considered under the terrorist property reporting guidelines but determined not to be reportable, including the reasons why the transaction or property was not reported;
- Documentation, memorandums, and copies of the reports filed for all terrorist property reports filed with FINTRAC or the RCMP and CSIS;
- Documentation and memorandums for all transactions considered under the cross-border currency or monetary instrument reporting guidelines but determined not to be reportable, including the reasons why the transaction was not reported;
- Documentation, memorandums, and copies of the report filed for all CCMIRs filed with CBSA; and

- Documentation regarding any and all compliance reviews conducted internally or by outside consultants, including any memorandums from the senior partners/shareholders regarding corrective action needed to be taken.

Procedure 3* —** The compliance officer will ensure that only ***required information is maintained in the compliance file. The CGA *Canada Code of Ethical Principles and Rules of Conduct* (CEPROC) allows the practitioner to report client information that is ***required*** to be reported by Statute. Only information that is ***required*** may be reported without breaching the CEPROC; ***no voluntary information is to be included in the compliance file***.

Procedure 4 — The compliance file will be maintained by the compliance officer or his/her designate if the compliance officer is not available.

Procedure 5 — The compliance file will be maintained in paper format so that it can be readily produced if requested by FINTRAC.

The compliance file and related documentation can be kept in electronic format provided that a paper copy can be readily produced if requested by FINTRAC and also provided that an electronic signature of the individual who must sign the reports filed is also retained.

***Procedure 6* —** The compliance officer will ensure that the respective contents in the compliance file are maintained for a period of at least five years following the date each record was created.

5.7 Client communication

5.7.1 *Prohibited disclosure*

The *Act* states that it is an offence to disclose to a client that a CGA firm has made a suspicious transaction report with the intent to prejudice a criminal investigation (whether such investigation has been started yet or not). This provision of being dependent upon the "intent to prejudice a criminal investigation" is intended to relieve CGA firms of liability in the case of accidental disclosure. It should be the policy of the CGA firm that no responsible partners/shareholder, professional staff, other staff members, agents, or anyone else working on behalf of the firm shall disclose to any client that a suspicious transaction report has been considered or filed.

5.7.2 *Notification to clients*

It should be the policy of the CGA firm to notify all clients of the statutory obligations to report suspicious transactions, large cash transactions, terrorist property, and cross-border currency or monetary instruments.

Notification to clients lets them know that the CGA firm may have to report various types of transactions and activities. This is a preventative policy that is designed to help prevent the firm from being used by an unscrupulous client.

5.7.3 *Engagement letters*

The following should be added to all engagement letters:

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* places legal requirements on [*CGA firm*] to report transactions that may be suspicious of being related to a money laundering or terrorist financing offence. It also requires our firm to report large cash transactions that exceed $10,000, the cross-border of currency or monetary instruments that exceed $10,000, and whether we are in possession or control of property that is considered terrorist property. Finally, the *Act* requires our firm to ascertain the identity and existence of clients and other entities. To meet these obligations, [*CGA firm*] may have to report information about you [*the company*] that might otherwise be confidential. The reporting of this information may place you [*the company*] and this firm in a conflict of interest. Should such a conflict arise, this firm may be required to withdraw from this engagement. Please be advised that we will do everything in our power to avoid such conflicts and that only information that is required will be disclosed. You hereby acknowledge this legal requirement placed upon this firm and the potential conflict of interest that may arise as a result of it. You also hereby authorize this firm to release and disclose information related to you [*the company*] when required by statute to do so.

5.7.4 *Representation letters*

The following should be added to all representation and transmittal letters:

We hereby acknowledge that [*CGA firm*] have made us aware of your legal obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. We hereby acknowledge that we are aware of potential conflict of interest that may arise as a result of your legal obligations under this *Act* and authorize [*CGA firm*] to release and disclose information about [*company name*] as required by statute.

5.8 Compliance reviews and search and seizure by FINTRAC or other authorities

The *Act* contains provisions that give FINTRAC the authority to ensure firms are in compliance with the *Act*. It stipulates that any person authorized by FINTRAC has the power to enter a firm's premises without a search warrant at any reasonable time to determine whether the firm, the professional staff, other staff members, agents, and anyone else authorized to act on behalf of the firm are complying with the obligations of the legislation.

In the course of a compliance search, every member of the firm is required to give the person authorized by FINTRAC:

- 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;
- The right to use any copying equipment to make any required copies;
- All reasonable assistance to enable them to carry out their responsibilities, and
- Any information with respect to the administration of the reporting and recording obligations that they may reasonably require.

Should it become apparent that a person authorized by FINTRAC has entered the firm's premises, the subsequent procedures should be followed:

Procedure 1 — The member of the firm who first becomes aware of the person's entry will request identification from the authorized person.

Procedure 2 — The member of the firm who requests the identification will then immediately inform the compliance officer that a person authorized by FINTRAC has entered the firm's premises.

Procedure 3 — The compliance officer will be responsible for liaising with the person authorized by FINTRAC throughout the course of the compliance search and will arrange for all assistance requested by that person.

Procedure 4 — All members of the firm who are requested to provide assistance will ensure the compliance officer is present and will provide the FINTRAC authorized person with the assistance requested provided it is within the framework of what is required of them as per above.

Procedure 5 — Should the FINTRAC-authorized person identify documents or files that he/she wants to review or copy, the compliance officer must establish whether legal privilege can be attached to the documents or files. If it can, the compliance officer will contact the respective lawyer for the file, who will exert the claim of privilege on those documents. (See section 5.8.1 for information on privileged documents). If the documents and files cannot have privilege claimed, they will be provided to the FINTRAC-authorized person.

Procedure 6 — The compliance officer will keep a record in the compliance file of any searches and seizures made, and will record whether any documents or files were removed from the firm's premises. The compliance officer will have the FINTRAC-authorized person sign the record of what documents were removed.

5.8.1 *Claiming privilege on seized client documents*

The firm may have client documents and files that are a work product that a lawyer can claim solicitor-client privilege over. Under the *Act,* the person authorized by FINTRAC is not entitled to examine or make copies of documents for which a lawyer has solicitor-client privilege in respect of the document. If, during the course of the FINTRAC review or search and seizure, the compliance officer believes documents or files identified by the FINTRAC-authorized person may have privilege claimed on them, the subsequent procedures should be followed:

Procedure 1 — The compliance officer must identify to the FINTRAC-authorized person that he/she believes the document or file may have solicitor-client privilege attached to it.

Procedure 2 — The compliance officer will attempt to contact the respective lawyer for the document or file immediately so that the lawyer may assert the privilege.

Procedure 3 — If the compliance officer is unable to contact the lawyer immediately, he/she will request a short period of time be provided to allow for consultation with the respective lawyer. The *Act* states that the FINTRAC-authorized person must give a "reasonable opportunity" for the person (compliance officer or other person) to contact the legal counsel to enable a claim of solicitor-client privilege to be made.

Procedure 4 — The compliance officer will make a record of any documents or files where solicitor-client privilege has been claimed and will follow the legal counsel's instructions on what to do with the respective documents or files.

Procedure 5 — Pursuant to legal counsel's instructions, the compliance officer, in accordance with the *Act,* will place the documents or files in a package and seal and identify the package. The compliance officer will then retain the sealed or marked documents or files and ensure that it is preserved until it is produced to a judge as required under the *Act* and an order is issued in respect of the documents or files.

6. Penalties for non-compliance

The breaches and their respective maximum penalties are:

- Failure to file a suspicious transaction report (STR) — up to five years in jail and/or a fine of $2,000,000 (s.75);
- Failure to file a large cash transaction report (LCTR) — $500,000 for first offence and $1,000,000 for each subsequent offence (s.77);
- Failure to file a terrorist property report (TPR) — up to five years in jail and/or a fine of up to $2,000,000 (s.75);
- Failure to maintain a record of large cash transactions — $500,000 for first offence and $1,000,000 for each subsequent offence (s.77);
- Failure to retain required records — up to five years in jail and/or fine of $500,000 (s.74);
- Failure to implement a compliance regime — up to five years in jail and/or a fine of $500,000 (s.74);
- Disclosing the fact that an STR has been made with the intent to prejudice a criminal investigation — up to two years in jail (s.76);
- Failure to assist in a compliance review — up to five years in jail and/or fine of $500,000 (s.74); and
- Failure to cooperate with a Customs officer regarding currency or monetary instrument reporting — up to five years in jail and/or fine of $500,000 (s.74).

7. Review of compliance policies and procedures

The review of the compliance regime and its policies and procedures is required under the regulations. It will allow the firm to monitor the effectiveness of the compliance regime and evaluate the need to modify existing policies and procedures, if necessary, or to implement new ones. The review must be conducted at least once every two years.

The regulations require the review to be conducted by either internal or external auditors. If the firm does not have internal or external auditors, the Senior partners/shareholders, excluding the compliance officer, will appoint a person(s) within the firm to conduct the review (compliance reviewer).

The compliance reviewer must be independent of the reporting, record-keeping, and compliance-monitoring functions. If the senior partners/shareholders cannot identify a person(s) within the firm to conduct the review, an outside consultant should be retained to do it.

7.1 Review procedures

When conducting the "self-review" of the firm's compliance regime and its policies and procedures, these procedures should be followed:

Procedure 1 — The compliance reviewer will undertake to conduct the review at least once every two years.

Procedure 2 — The compliance reviewer will interview, as is considered necessary, partners/shareholders, professional staff, other staff, agents, and anyone else authorized to act on behalf of the firm to determine their knowledge of the legislative requirements and the firm's policies and procedures.

Procedure 3 **—** The compliance reviewer will conduct a sampling of large cash transactions, if any, followed by a review of the reporting of such transactions.

Procedure 4 **—** The compliance reviewer will review the criteria and process for identifying suspicious transactions reporting, terrorist property reporting, and cross-border currency or monetary instruments reporting.

Procedure 5 **—** The compliance reviewer will test the validity and reasonableness of exceptions to reporting that may have been granted.

Procedure 6 — The compliance reviewer will conduct a test of the record-keeping system for compliance with the legislation.

Procedure 7 — The compliance reviewer will document the scope and results of the review. Deficiencies should be identified and reported to the senior partners/shareholders within 30 days of completion of the review and a request for a response indicating corrective actions and a timeline for implementing such actions. A copy of the report should be placed in the compliance file.

Procedure 8 — The senior partners/shareholders should provide a written memorandum to the compliance officer indicating a corrective action plan and timelines for implementation should deficiencies be found in the review. A copy of this memorandum will be maintained in the compliance file. If it has been determined that the risk is high for money laundering or terrorist financing, the organization will have to take measures to mitigate the risk, take reasonable measures to keep client information up to date, and conduct ongoing monitoring of financial transactions to detect suspicious transactions.

These reviews do not have to be submitted to FINTRAC. If FINTRAC inquires into the compliance program, the report can be used to substantiate the existence and effectiveness of the program.

7.2 When review of policies and procedures will take place

The review of the compliance regime will take place at least once every two years. The firm should also undertake an additional review in the following circumstances:

- when there are changes in legislation,

- when the compliance officer becomes aware that the firm has not been in compliance with the policies and procedures, and
- if the firm begins to provide a new service.

The compliance officer is responsible for monitoring the legislation for changes that might trigger a need to review the compliance policies and procedures.

8. Keeping current with changes in the legislation

Part of maintaining a compliance manual is staying current with the legislation. The compliance officer is responsible for ensuring that the most up-to-date legislation, including regulations, is part of this compliance manual. In order to keep current with the legislation, these procedures should be followed:

Procedure 1 — The compliance officer should check the website of FINTRAC at http://www.fintrac.gc.ca on a quarterly basis. Updates to the legislation can generally be found under the "what's new" heading.

Procedure 2 — The compliance officer should ensure that any updates to the legislation or regulations are communicated to all partners/shareholders, professional staff, other staff, agents, and anyone else who is authorized to act on behalf of the firm. This communication may take place by way of memorandum, seminar, or any other means considered necessary by the compliance officer to ensure the updates are understood.

Procedure 3 — The compliance officer should update the compliance manual as necessary to reflect any changes/updates to the legislation or regulations. This will include the modification or creation of new policies and procedures if necessary to ensure the firm is in compliance.

Procedure 4 — The compliance officer should maintain a log of all searches made for updates, the results of those searches, and updates/changes made to the compliance manual. This log will be kept in the back of the compliance manual.

9. Current legislation

A copy of the most up-to-date version of the *Act*, Regulations, and Guidelines should be kept in the compliance manual. The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, Regulations, and FINTRAC's Guidelines can be obtained at http://www.fintrac.gc.ca.