

UPDATE ON CANADA'S 2008 ANTI-MONEY LAUNDERING REQUIREMENTS FOR CAs

Chartered accountants and accounting firms 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 to identify clients, report suspicious transactions, keep detailed records, report large cash transactions and electronic fund transfers, and implement a compliance program (see Exhibit 1).

Significant amendments to Canada's anti-money laundering (AML) and terrorist financing laws come into effect on June 23, 2008, followed by even more changes later this year. This article highlights some of the more important new AML regulations, particularly those that may have an impact on chartered accountants and accounting firms. It provides an overview of the changing Canadian and international environments, explains how reporting entities will be affected, reviews the risk-based approach for implementing a compliance program and stresses the need to keep up with new developments.

Changing Canadian and international environments

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.

Exhibit 1

Activities that trigger AML obligations for CAs and CA firms

Since 2001, Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)* has required that chartered accountants and accounting firms implement a compliance program if they engage in any of the following **triggering activities** on behalf of any person or entity (other than an employer) or give instructions in respect of those activities on behalf of any person or entity (other than an employer):

- receiving or paying funds (for example, making GST payments or receiving GST refunds on behalf of clients);
- purchasing or selling securities, real property or business assets or entities (for example, giving instructions regarding client investments as part of wealth management activities); or
- transferring funds or securities by any means (for example, having authority to transfer funds to a client's payroll account even if that authority applies only when a client is on holidays).

The *PCMLTFA* requirements apply even if the triggering activities are carried out on a volunteer basis. However, the requirements **do not apply** to:

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

Since the *PCMLTFA* first came into force, the domestic and international environment has changed. First, 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 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 FINTRAC proposed amendments to help them better fulfill their mandates. Third, some financial institutions and financial intermediaries requested changes 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. Many amendments come into force on June 23, 2008.

More reporting entities subject to *PCMLTFA*

The amended *PCMLTFA* requires reporting entities — financial institutions and financial intermediaries — to identify their customers, keep certain records, report large cash transactions and international electronic fund transfers to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and develop an internal control compliance program. Reporting entities include banks, cooperative credit societies, savings and credit unions, caisses populaires, life insurance companies, life insurance brokers or agents, trust and loans companies, securities dealers, money services businesses (including foreign exchange dealers), casinos, real estate brokers or sales representatives, and accountants or accounting firms. The legal profession, dealers in precious metals and stones, and real estate developers will also become reporting entities.

Additional AML requirements

Commencing June 23, 2008, chartered accountants and accounting firms carrying out triggering activities (see Exhibit 1) must meet expanded *PCMLTFA* requirements for reporting, record keeping and client identification. For example, they will have to report attempted suspicious transactions to FINTRAC; keep a record of every receipt in excess of \$3,000 (whether cash on not); and implement enhanced procedures to identify clients.

In addition, the requirements for a compliance program have been expanded to include the following five elements that are crucial for an effective system of internal controls:

- the appointment of a compliance officer;
- the development and application of written compliance policies and procedures that are approved by a senior officer and kept up to date;
- an assessment and documentation of risks related to money laundering and terrorist financing;
- a documented and maintained training program for employees or agents;
- a review, at least every two years, of the effectiveness of the compliance policies and procedures, the assessment of risks related to money laundering and terrorist financing and the training program.

Taking a risk-based approach

Perhaps the most difficult part of implementing an effective compliance program is building in a risk-based approach for detecting and dealing with potential money laundering and terrorist financing. This risk assessment applies to chartered accountants and accounting firms themselves, as well as to their clients.

FINTRAC elaborates on the risk-based approach in *Guideline 4 — Implementation of a Compliance Regime* (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 help complete the risk assessment, FINTRAC suggests referring to *Guideline 1: Backgrounder* for additional information on money laundering and terrorist financing and to *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 that particular entity by considering:

- clients and business relationships;
- products, services and delivery channels;
- geographic areas where the services are provided or where clients are located.

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.”

According to *Guideline 4* (paragraph 6.4), ongoing monitoring is essential: “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.”

High price of non-compliance

Failure to comply with the new *PCMLTFA* requirements can lead to criminal charges and severe penalties, for example:

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

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. For example, FINTRAC has recently updated several Guidelines that are of particular relevance to chartered accountants and accounting firms:

- *Guideline 2 — Suspicious Transactions*, dated March 2008 (effective June 23, 2008);
- *Guideline 4 — Implementation of a Compliance Regime*, dated February 2008 (effective June 23, 2008);
- *Guideline 6D — Record Keeping and Client Identification for Accountants*, dated February 2008 (effective June 23, 2008).

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 on current activities and publications by regularly visiting the FINTRAC website (<http://www.fintrac-canafe.gc.ca/>) and the CICA's Online Anti-Money Laundering Resource Centre (http://www.cica.ca/index.cfm/ci_id/2081/la_id/1.htm).

Howard Wasserman, CA●CIRP, CFE, CFI is a trustee in bankruptcy and consultant on forensic investigations, insolvency, restructuring and white collar crime. He is the chair of the CICA's Anti-Money Laundering Advisory Committee.

Paul-Émile Roy, CA, is a principal in the CICA's Research Studies department. He provides staff support to the Anti-Money Laundering Advisory Committee.