Financial Transactions and Reports Analysis Centre of Canada
Centre d'analyse des opérations et déclarations financières du Canada

Guideline 4: Implementation of a Compliance Regime

Rev. 2016-06

Canada

Guideline 4: Implementation of a Compliance Regime

July 2016

This replaces the previous version of *Guideline 4: Implementation of a Compliance Regime* issued in June 2015. The changes made are indicated by a side bar to the right of the modified text in the PDF version.

Table of Contents

1 General

The objective of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act) is to help detect and deter money laundering and the financing of terrorist activities. It is also to facilitate investigations and prosecutions of money laundering and terrorist activity financing offences. This includes implementation of reporting, record keeping, client identification and compliance regime requirements for individuals and entities described in section 2.

If you are such an individual or entity, this guideline has been prepared to help you implement your compliance regime intended to ensure compliance with your reporting, record keeping and client identification obligations.

This guideline uses plain language to explain the most common situations under the Act as well as the related regulations. It is provided as general information only. It is not legal advice, and as such, is not intended to replace the Act and Regulations.

For more information about money laundering, terrorist financing or other requirements under the Act and Regulations, see the guidelines in this series:

- *Guideline 1: Backgrounder* explains money laundering and terrorist financing and their international nature. It also provides an outline of the legislative requirements as well as an overview of FINTRAC's mandate and responsibilities.
- *Guideline 2: Suspicious Transactions* explains how to report a suspicious transaction. It also provides guidance on how to identify a suspicious transaction, including general and industry-specific indicators that may help when conducting or evaluating transactions.
- *Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC* explains when and how to submit suspicious transaction reports. There are two different versions of Guideline 3, by reporting method.
- *Guideline 4: Implementation of a Compliance Regime* explains the requirement for reporting entities to implement a regime to ensure compliance with their obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and associated regulations.
- *Guideline 5: Submitting Terrorist Property Reports to FINTRAC* explains when and how to submit a terrorist property report.
- *Guideline 6: Record Keeping and Client Identification* explains the requirement for reporting entities to ascertain the identity of their clients and keep records. There are several different versions of Guideline 6, with each one applicable to a particular sector.
- *Guideline 7: Submitting Large Cash Transaction Reports to FINTRAC* explains when and how to submit large cash transaction reports. There are two different versions of Guideline 7, by reporting method.

- *Guideline 8: Submitting Electronic Funds Transfer Reports to FINTRAC* explains when and how to submit electronic funds transfer reports. There are three different versions of Guideline 8, by report type and reporting method.
- *Guideline 9: Submitting Alternative to Large Cash Transaction Reports to FINTRAC* explains when and how financial entities can choose the alternative to large cash transaction reports. This is only applicable to financial entities.
- *Guideline 10: Submitting Casino Disbursement Reports to FINTRAC* explains when and how to submit casino disbursement reports. There are two different versions of Guideline 10, by reporting method.

If you need more help after you read this or other guidelines, call FINTRAC's national toll-free enquiries line at 1-866-346-8722.

Your compliance policies and procedures may cover situations other than the ones described in this guideline, for purposes other than your requirements under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. For example, the federal or provincial regulator for your sector may require you to apply additional compliance policies and procedures other than what is described in this guideline.

2 Who Has to Implement a Compliance Regime?

If you are one of the following individuals or entities (called reporting entities), you have to implement a compliance regime intended to ensure compliance with your reporting, record keeping and client identification requirements.

2.1 Financial entities

Financial entities are banks (that is, those listed in Schedule I or II of the *Bank Act*) or authorized foreign banks with respect to their operations in Canada, credit unions, caisses populaires, financial services cooperatives, credit union centrals (when they offer financial services to anyone other than a member entity of the credit union central), trust companies, loan companies or agents of the Crown that accept deposit liabilities.

Foreign Branches or Foreign Subsidiaries

If you are a financial entity, that has foreign branches or foreign subsidiaries which carry out activities similar to those of a financial entity, securities dealer or insurance broker; and that are wholly owned by you or have consolidated financial statements with you, you have the following requirements:

- Develop policies to establish requirements with respect to record keeping and their retention, and ascertain client identity.

- Establish and implement a compliance program which must also include the risk assessment of money laundering or a terrorist activity financing

offence, and risk mitigation controls when the risk is considered to be high. These requirements must be similar to those in Canada. Please refer to section 3 of this document for further information on the five elements required for a compliance regime.

If you have a Board of Directors, it shall approve these policies.

You must ensure that your foreign branches or foreign subsidiaries apply these policies to the extent it is permitted by the laws of the country in which the foreign subsidiary or foreign branch is located. If they cannot implement these policies or part of them because they conflict with the laws of the country in which they are located, you must keep a record including the reasons why these policies cannot be implemented and provide a copy, within a reasonable time period, to your regulating body and FINTRAC.

Exceptions to definition of Foreign Subsidiaries

These requirements do not apply to you if:

- You are an authorized foreign bank within the meaning of section 2 of the *Bank Act* or an agent of the crown that accepts deposit liabilities;
- You are a foreign subsidiary of a Canadian entity that has developed policies that establish record keeping, client identity, and compliance requirements similar to sections 6, 6.1, and 9.6 of the *PCMLTF Act* and you apply these policies developed by the Canadian entity in accordance with Canadian laws and the laws of the country in which you (the foreign subsidiary) are located.
- You are a Canadian subsidiary of a foreign entity that has developed policies that establish record keeping, client identity, and compliance requirements similar to sections 6, 6.1, and 9.6 of the *PCMLTF Act* and you apply these policies developed by the foreign entity in accordance with Canadian laws.

Information Exchange between Domestic and Foreign Affiliated Entities

If you are a financial entity that is affiliated with another entity or a foreign entity that carries out activities similar to those of a financial entity, securities dealer or insurance company, you must develop and apply policies and procedures in relation to the exchange of information between you and your affiliated entities. The purpose of this exchange of information is to help detect and deter money laundering and the financing of terrorist activities and to assess the risk of such an offence.

As part of your risk assessment, you may want to keep a record including the rationale as to why these policies cannot be implemented by the affiliated entities.

Affiliated entity means if one of you is wholly owned by the other, if both of you are wholly owned by the same entity or if your financial statements are consolidated.

See *Guideline 6G: Record Keeping and Client Identification for Financial Entities* for more information.

2.2 Life insurance companies, brokers and agents

A life insurance company means one regulated by provincial legislation, or a life company or foreign life company under the *Insurance Companies Act*. A life insurance broker or agent means an individual or entity that is registered or licensed provincially to carry on the business of arranging contracts of life insurance.

If you are employed by an individual or entity who is also subject to these requirements, your employer is responsible for the compliance regime. For example, when life insurance agents are employees of a life insurance company, the compliance regime requirement is the responsibility of the life insurance company. If you are a life insurance broker or independent agent (that is, you are not an employee), you are responsible for your own compliance regime.

Foreign Branches or Foreign Subsidiaries
If you are a life insurance company that has foreign branches or foreign subsidiaries which carry out activities similar to those of a financial entity, securities dealer or insurance company; and that are wholly owned by you or have consolidated financial statements with you, you have the following requirements:

- Develop policies to establish requirements with respect to record keeping and retention, and ascertain client identity.

- Establish and implement a compliance program which must also include the risk assessment of money laundering or terrorist activity financing offence, and risk mitigation controls when the risk is considered to be high. These requirements must be similar to those in Canada. Please refer to section 3 of this document for further information on the five elements required for a compliance regime.

If you have a Board of Directors, they shall approve these policies

You must ensure that your foreign branches or foreign subsidiaries apply these policies to the extent it is permitted by the laws of the country in which the foreign subsidiary or foreign branch is located. If they cannot implement these policies or

part of them because they conflict with the laws of the country in which they are located, you must keep a record including the reasons why these policies cannot be implemented and provide a copy, within a reasonable time period, to your regulating body and FINTRAC.

Exceptions to definition of Foreign Subsidiaries

These requirements do not apply to you if you are a foreign company within the meaning of section 2 of the *Insurance Companies Act.*

These requirements do not apply to subsidiaries of foreign subsidiaries. For example, if Insurance Company A has a foreign subsidiary (Subsidiary A) and there is a Subsidiary B of Subsidiary A, then these requirements do not apply to Subsidiary B.

These requirements do not apply to you if you are the Canadian subsidiary of a foreign entity, when the foreign entity has developed policies that are similar to Canada's compliance regime requirements (see section 3 of this guideline) and also have in place policies to assess the risk of money laundering and terrorist activity financing. For example, when Foreign Bank A with subsidiaries A and B in Canada already has policies regarding client identification, record keeping and the establishment of a compliance regime, then these requirements do not apply to the Canadian subsidiaries A and B. See *Guideline 6A: Record Keeping and Client Identification for Life Insurance Companies, Brokers and Agents* for more information.

Information Exchange between Domestic and Foreign Affiliated Entities

If you are a life insurance company that is affiliated with another entity or a foreign entity that carries out activities similar to those of a financial entity, securities dealer or insurance company, you must develop and apply policies and procedures in relation to the exchange of information between you and your affiliated entities. The purpose of this exchange of information is to help detect and deter money laundering and the financing of terrorist activities and to assess the risk of such an offence.

As part of your risk assessment, you may want to keep a record including the rationale as to why these policies cannot be implemented by the affiliated entities.

Affiliated entity means if one of you is wholly owned by the other, if both of you are wholly owned by the same entity or if your financial statements are consolidated.

2.3 Securities dealers

A securities dealer is an individual or entity authorized under provincial legislation to engage in the business of dealing in securities or any other financial instruments or to provide portfolio management or investment advising services, other than persons who act exclusively on behalf of such an authorized person or entity. This means that if you are an individual who is authorized to deal in securities or any other financial instruments, but you do so **exclusively** on behalf of another entity or individual who is a securities dealer, you are not considered to be a securities dealer under this definition.

In addition, if you are an employee of an individual or entity who is also subject to these requirements, your employer is responsible for the compliance regime. For example, if you are an employee of an entity engaged in the business of dealing in securities, the compliance regime requirement is the responsibility of the entity.

Similarly, if you are an agent of (or you are authorized to act on behalf of) an individual or entity who is also subject to these requirements, that other individual or entity is responsible for the compliance regime.

Foreign Subsidiaries or Foreign Branches

If you are a securities dealer that has foreign branches or foreign subsidiaries which carry out activities similar to those of a financial entity, securities dealer or insurance company; and that are wholly owned by you or have consolidated financial statements with you, you have the following requirements:

- Develop policies to establish requirements with respect to record keeping and retention, and ascertain client identity.
- Establish and implement a compliance program which must also include the risk assessment of money laundering or terrorist activity financing offence, and risk mitigation controls when the risk is considered to be high. These requirements must be similar to those in Canada. Please refer to section 3 of this document for further information on the five elements required for a compliance regime.

If you have a Board of Directors, they shall approve these policies.

You must ensure that your foreign branches or foreign subsidiaries apply these policies to the extent it is permitted by the laws of the country in which the foreign subsidiary or foreign branch is located. If they cannot implement these policies or part of them because they conflict with the laws of the country in which they are located, you must keep a record including the reasons why these policies cannot be implemented and provide a copy, within a reasonable time period, to your regulating body and FINTRAC.

Exceptions to definition of Foreign Subsidiaries

These requirements do not apply to subsidiaries of foreign subsidiaries. For example, if Securities Dealer A has a foreign subsidiary (Subsidiary A) and there is a Subsidiary B of Subsidiary A, then these requirements do not apply to Subsidiary B.

These requirements do not apply to you if you are the Canadian subsidiary of a foreign entity, when the foreign entity has developed policies that are similar to Canada's compliance regime requirements (see section 3 of this guideline) and also have in place policies to assess the risk of money laundering and terrorist activity financing. For example, when Foreign Company A with subsidiaries A and B in Canada already has policies regarding client identification, record keeping and the establishment of a compliance regime, then these requirements do not apply to the Canadian subsidiaries A and B. See *Guideline 6E: Record Keeping and Client Identification for Securities Dealers* for more information.

Information Exchange between Domestic and Foreign Affiliated Entities

If you are a securities dealer that is affiliated with another entity or a foreign entity that carries out activities similar to those of a financial entity, securities dealer or insurance company, you must develop and apply policies and procedures in relation to the exchange of information between you and your affiliated entities. The purpose of this exchange of information is to help detect and deter money laundering and the financing of terrorist activities and to assess the risk of such an offence.

As part of your risk assessment, you may want to keep a record including the rationale as to why these policies cannot be implemented by the affiliated entities.

Affiliated entity means if one of you is wholly owned by the other, if both of you are wholly owned by the same entity or if your financial statements are consolidated.

2.4 Casinos

Casinos are those authorized by a Canadian provincial, territorial or federal government to do business and that conduct their business in a permanent establishment. It only includes those where roulette or card games are played in the establishment, or where there is a slot machine. For these purposes, a slot machine does not include a video lottery terminal.

Registered charities may be authorized to carry on business temporarily as a casino for charitable purposes. If this type of business is carried out in the establishment of a casino for no more than two consecutive days at a time under the supervision of the casino, the activities are considered to be the supervising casino's. In this case, the supervising casino is responsible for the compliance regime as well as the other requirements and obligations.

2.5 Real estate

Real estate brokers or sales representatives
Real estate brokers or sales representatives are individuals or entities that are registered or licensed in a province to sell or purchase real estate. They have to implement a compliance regime when they act as an agent regarding the purchase or sale of real estate. This includes the buying or selling of land, buildings, houses, etc.

If you are a real estate broker or sales representative, this requirement does not apply to you for activities related to property management. This means that if you only deal in property management transactions, such as leases or rental management, not purchases or sales, the compliance regime requirement explained in this guideline do not apply to you.

If you are an employee of an individual or entity who is also subject to these requirements, your employer is responsible for the compliance regime. For example, if you are a sales representative who is an employee of a real estate broker, the compliance regime requirement is the responsibility of the broker.

Real estate developers
A real estate developer means an individual or an entity other than a real estate broker or sales representative, who in any calendar year after 2007 has sold one of the following to the public:

- at least five new houses or condominium units;
- at least one new commercial or industrial building;
- at least one new multi-unit residential building each of which contains five or more residential units; or
- at least two new multi-unit residential buildings that together contain five or more residential units.

If you are a real estate developer, you have to implement a compliance regime if you sell any of the following to the public:

- a new house;
- a new condominium unit;
- a new commercial or industrial building; or
- a new multi-unit residential building.

If you are an entity that is a corporation, you are subject to this whether you sell those buildings on your own behalf or on behalf of a subsidiary or affiliate. In this context, an entity is affiliated with another entity if one of them is wholly-owned by the other, both are wholly-owned by the same entity or their financial statements are consolidated.

2.6 Agents of the Crown

Agents of the Crown are government departments or agents of her Majesty in right of Canada or of a province. If you are an agent of the Crown that sells or redeems money orders in the course of providing financial services to the public, you are subject to the compliance regime requirement explained in this guideline.

If you accept deposit liabilities in the course of providing financial services to the public, such as a provincial savings office, you are considered a financial entity (see subsection 2.1).

If you are an agent of the Crown that sells precious metals to the public, you are considered a dealer in precious metals and stones (see subsection 2.9).

2.7 Money services businesses

A money services business means an individual or entity engaged in the business of any of the following activities:

- foreign exchange dealing;
- remitting or transmitting funds by any means or through any individual, entity or electronic funds transfer network; or
- issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments. This does not include redeeming cheques payable to a named individual or entity. In other words, cashing cheques made out to a particular individual or entity is not included.

Money services businesses also include alternative money remittance systems such as Hawala, Hundi, Chitti, etc.

If you are an employee of a money services business, it is your employer who is engaged in the business and therefore responsible for the compliance regime. If you are an agent of (or you are authorized to act on behalf of) another individual or entity that is a money services business, that other individual or entity is responsible for the compliance regime for the relevant activities that you perform on their behalf.

2.8 Accountants and accounting firms

An accountant means a chartered accountant, a certified general accountant, a certified management accountant or a certified professional accountant. An

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

If you are an accountant or an accounting firm, you have to implement a compliance regime if you engage in any of the following activities on behalf of any individual or entity (other than your employer) or give instructions in respect of those activities on behalf of any individual or entity (other than your employer):

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

You are subject to this whether or not you receive professional fees for these activities. However, you are not subject to this regarding the professional fees themselves.

The activities listed above do not include audit, review or compilation engagements carried out according to the recommendations in the Canadian Institute of Chartered Accountants (CICA) Handbook.

Giving advice to a client, in the context of your accountant-client relationship, is not considered providing instructions. If you need further clarification about this, refer to FINTRAC Interpretation Notice No. 2.

Providing bankruptcy services or acting as an insolvency practitioner does not trigger reporting obligations. If you need further clarification about this, refer to FINTRAC Interpretation Notice No. 7.

If you are an employee of an individual or entity who is also subject to these requirements, your employer is responsible for the compliance regime. For example, if you are an accountant who is an employee of an accounting firm, the compliance regime requirement is the responsibility of the firm.

Similarly, if you are an agent of (or you are authorized to act on behalf of) an individual or entity who is also subject to these requirements, that other individual or entity is responsible for the compliance regime.

2.9 Dealers in precious metals and stones

A dealer in precious metals and stones (DPMS) means an individual or an entity that buys or sells precious metals, precious stones or jewellery, in the course of its business activities. Precious metals include gold, silver, palladium or platinum whether in coins, bars, ingots, granules or in any other similar form. Precious stones include diamonds, sapphires, emeralds, tanzanite, rubies or alexandrite.

Jewellery means objects made of precious metals, precious stones or pearls intended for personal adornment.

If you are a DPMS, you have to implement a compliance regime if you engage in the purchase or sale of precious metals, precious stones or jewellery in an amount of $10,000 or more in a single transaction. However, you are not subject to this when you engage in a purchase or sale carried out for, in connection with, or for the purpose of manufacturing jewellery, extracting precious metals or precious stones from a mine, or cutting or polishing precious stones.

An agent of the Crown (that is, a government department or an agent of her Majesty in right of Canada or of a province) is considered to be a DPMS, when it sells precious metals to the public in an amount of $10,000 or more in a single transaction.

2.10 British Columbia notaries

A British Columbia notary means a British Columbia notary public or a British Columbia notary corporation. In this context, a notary public means an individual who is a member of the Society of Notaries Public of British Columbia. Also in this context, a notary corporation means an entity that provides notary services to the public in British Columbia under the *Notaries Act* of that province.
If you are a British Columbia notary, you have to implement a compliance regime if you engage in any of the following activities on behalf of any individual or entity (other than your employer), or give instructions on behalf of any individual or entity (other than your employer):

- receiving or paying funds (other than those received or paid for professional fees, disbursements, expenses or bail);
- purchasing or selling securities, real estate or business assets or entities; or
- transferring funds or securities by any means.

3 What is a Compliance Regime?

The implementation of a compliance regime is a legislative requirement and a good business practice for anyone subject to the Act and its regulations. A well-designed, applied and monitored regime will provide a solid foundation for compliance with the legislation. As not all individuals and entities operate under the same circumstances, your compliance regime will have to be tailored to fit your individual needs. It should reflect the nature, size and complexity of your operations.

If you are a member of an association within your sector of activity, you may wish to check with them to find out if any information sharing about any aspect of compliance regime implementation is available. You may also check with any regulatory body covering your sector in this regard.

Your compliance regime has to include the following:

- the appointment of a compliance officer (see section 4);
- the development and application of compliance policies and procedures. These policies and procedures have to be written and kept up to date. If you are an entity, they also have to be approved by a senior officer (see section 5);
- an assessment and documentation of risks related to money laundering and terrorist financing, as well as the documentation and implementation of mitigation measures to deal with those risks (see section 6);
- if you have employees or agents or any other individuals authorized to act on your behalf, an ongoing compliance training program for them. The training program has to be in writing and maintained (see section 7); and
- a review of your compliance policies and procedures to test their effectiveness. The review has to cover your policies and procedures, your assessment of risks related to money laundering and terrorist financing and your training program. The review also has to be done every two years (see section 8).

These five elements are key to any effective system of internal controls.

4 Appointment of a Compliance Officer

The individual you appoint will be responsible for the implementation of your compliance regime. Your compliance officer should have the authority and the resources necessary to discharge his or her responsibilities effectively. Depending on your type of business, your compliance officer should report, on a regular basis, to the board of directors or senior management, or to the owner or chief operator.

If you are a small business, the appointed officer could be a senior manager or the owner or operator of the business. If you are an individual, you can appoint yourself as compliance officer or you may choose to appoint another individual to help you implement a compliance regime.

In the case of a large business, the compliance officer should be from a senior level and have direct access to senior management and the board of directors. Further, as a good governance practice, the appointed compliance officer in a large business should not be directly involved in the receipt, transfer or payment of funds.

For consistency and ongoing attention to the compliance regime, your appointed compliance officer may choose to delegate certain duties to other employees. For example, the officer may delegate an individual in a local office or branch to ensure that compliance procedures are properly implemented at that location.

However, where such a delegation is made, the compliance officer retains responsibility for the implementation of the compliance regime.

5 Compliance Policies and Procedures

An effective compliance regime includes policies and procedures and shows your commitment to prevent, detect and address non-compliance. Your compliance program has to include written policies and procedures to assess the risks related to money laundering and terrorist financing in the course of your activities.

The level of detail of these policies and procedures depends on your needs and the complexity of your business. It will also depend on your risk of exposure to money laundering or terrorist financing. See section 6 for more information on risk-based approach.

For example, the compliance policies and procedures of a small business may be less detailed and simpler than those of a large bank. However, your policies and procedures have to be in writing and be kept up to date, whether you are a small business, an individual or an entity. Several factors could trigger the need to update, as often as necessary, your policies and procedures, such as changes in legislation, non-compliance issues, or new services or products.
In addition, if you are an entity, your policies and procedures also have to be approved by a senior officer. A senior officer of an entity includes its director, chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, as well as any individual who performs any of those functions. It also includes any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer.

It is important that your compliance policies and procedures are communicated, understood and adhered to by all within your business who deal with clients or any property owned or controlled on behalf of clients. This includes those who work in the areas relating to client identification, record keeping, and any of the types of transactions that have to be reported to FINTRAC. They need enough information to process and complete a transaction properly as well as to ascertain the identity of clients and keep records as required.

They also need to know when an enhanced level of caution is required in dealing with transactions, such as those involving countries or territories that have not yet established adequate anti-money laundering or anti-terrorist financing regimes consistent with international standards. See additional information about this in subsection 6.1.2 and the Guidance on the Risk-Based Approach to Combatting Money laundering and Terrorist Financing.

Your compliance policies and procedures should incorporate, at a minimum, the reporting, record keeping, client identification, risk assessment and risk mitigation

requirements applicable to you. For example, in the case of your reporting obligations relating to terrorist property or suspicions of terrorist financing, your policies and procedures should include the verification of related lists published in Canada. These are available on the Office of the Superintendent of Financial Institutions' website (http://www.osfi-bsif.gc.ca), by referring to the "Terrorist Listings and Sanctions" link.

Although directors and senior officers may not be involved in day-to-day compliance, they need to understand the statutory duties placed upon them, their staff and the entity itself.

6 Risk-Based Approach

For more detailed information on this element of your compliance regime, please consult the Guidance on the Risk-Based Approach to Combatting Money laundering and Terrorist Financing. Your compliance regime has to include an assessment and documentation of risks related to money laundering and terrorist financing in a manner that is appropriate to you. This is in addition to your client identification, record keeping and reporting requirements. A risk-based approach is a process that allows you to identify potential high risks of money laundering and terrorist financing and develop strategies to mitigate them.

Existing obligations, such as your client identification, will be maintained as a minimum baseline requirement. However, when it comes to situations where enhanced due diligence is appropriate, a principle of the risk-based approach is to focus your resources where they are most needed to manage risks within your tolerance level. You have to determine what is acceptable for you, taking into account the nature of each product or service, the geographical regions where you do your business and the relationships you have with your clients.

The approach to the management of risk and risk mitigation requires the leadership and engagement of senior management towards the detection and deterrence of money laundering and terrorist financing. Senior management is ultimately responsible for making management decisions related to policies, procedures and processes that mitigate and control the risks of money laundering and terrorist financing within a business.

What is a risk-based approach?
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 and business relationship information** up to date; and

- the **ongoing monitoring** of business relationships (for every sector except dealers in precious metals and stones, who only have to perform enhanced monitoring of high-risk business relationships).

These, as well as additional requirements for certain sectors, are explained in further detail in subsections 6.1 to 6.5.

6.1 Risk assessment

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.

While performing your risk assessment, you should refer to *Guideline 1: Backgrounder* for additional information on money laundering and terrorist financing and *Guideline 2: Suspicious Transactions* for additional common and industry-specific indicators related to your products and services as well as to occupation, business, financial history and past transaction patterns of your clients. These may help you in completing your risk assessment. Industry associations or regulators may also provide guidance that can be of assistance to you in this area.

You have to document and consider the following factors in your assessment:

- your products and services and the delivery channels through which you offer them;
- the geographic locations where you conduct your activities and the geographic locations of your clients;
- other relevant factors related to your business; and
- your clients and the business relationships you have with them.

You may want to perform the risk assessment for your business in two stages:

- Stage 1: Business-based risk assessment of your products, services, delivery channels and the geographic location in which your business operates.
- Stage 2: Relationships-based risk assessment of products and services your clients utilize as well as the geographic locations in which they operate or do business.

To help you assess products, services, delivery channels and geographic locations that may pose high risks of money laundering or terrorist financing, please consult the Guidance on the Risk-Based Approach to Combatting Money laundering and Terrorist Financing.

Similarly, for all clients within or outside of business relationships that may pose a high risk of money laundering or terrorist financing, we have included a list of the

most common risk indicators in the Guidance on the Risk-Based Approach to Combatting Money laundering and Terrorist Financing.

The Guidance on the Risk-Based Approach to Combatting Money laundering and Terrorist Financing provides examples to facilitate the assessment of the above factors. However, your risk assessment has to be appropriate for your specific business needs, which means that it may have to be more detailed than the checklists provided. You can customize the checklists or you can use a different method or another tool. For example, this could take the form of establishing clusters of clients with different risk variables (for example, products used, geographic location, transaction volumes, business industries engaged in, duration of the relationship, or other factors identified by your business). You could then give the separate clusters a weighting commensurate with the risk of potential money laundering and terrorist financing.

Your risk assessment may identify high-risk situations for which risk mitigation controls and monitoring may be required. See subsections 6.2 and 6.4 for more information.

Risk assessment requires good knowledge of your business operations and sound judgment exercised by your personnel so the risks for money laundering and terrorist financing can be weighed according to each individual factor as well as a combination of them. Your risk assessment is not static and will change over time. If you are a financial entity or a securities dealer, you have additional requirements related to risk assessment. See subsection 6.5 for more information.

6.1.1 Products, services and delivery channels

You have to be aware of and recognize products and services or combinations of them that may pose a high risk of money laundering or terrorist financing. Legitimate products and services can be used to mask illegal origins of funds, to move funds to finance terrorist acts or to hide the true identity of the actual owner or beneficiary of the product or service. Products and services that can support the movement and conversion of assets into, through and out of the financial system may pose a high risk. For example, these could include a money laundering related sale of high value goods that resulted in a cheque payable to a bearer which is then deposited into another individual’s account to make the transaction difficult to trace and detect.

In addition, you may also consider services identified by regulators, governmental authorities or other credible sources as being potentially high-risk for money laundering or terrorist financing. For example, international correspondent banking services, international private banking services, or services involving banknote and precious metal trading and delivery.

You have to consider, in a manner that is appropriate to you, the channels used to deliver your products or services. In today’s economy and global market, many

delivery channels do not bring the client into direct face-to-face contact with you (for example, Internet, telephone or mail), and are accessible 24 hours a day, 7 days a week, from almost anywhere. The more remote a client is from you, the more likely you will have to depend on a third party to deliver your products or services. The remoteness of some of these distribution channels can also be used to obscure the true identity of a client or beneficial owners and can therefore pose a high risk.

In addition, you should consider new or innovative services or delivery channels that you may use to deliver your products or services.

6.1.2 Geographic locations

You have to consider, in a manner that is appropriate to you, whether geographic locations in which you operate or undertake activities potentially pose a high risk for money laundering and terrorist financing. Depending on your business and operations, geographic locations can range from your immediate surroundings, whether rural or urban, to a province or territory, multiple jurisdictions within Canada (domestic) or other countries.

For example, large entities that operate in a number of domestic jurisdictions may refine the geographic locations factor to differentiate between urban locations having known higher crime rates in comparison to other urban or rural districts. Smaller entities that restrict their activities to a single geographic location or district may not need to make that distinction.

6.1.3 Other relevant factors

You need to consider, in a manner that is appropriate to you, any other factors that are relevant to you, your business or sector.

Guideline 1: Backgrounder and *Guideline 2: Suspicious Transactions* have more information about money laundering and terrorist financing that can help you in your risk assessment. You should also periodically review whether additional factors have become relevant to your situation, like risks arising from innovative or emerging technologies.

6.1.4 Clients within and clients outside of business relationships

The guidance below does not prohibit you from engaging in transactions with potential clients but provides you with information to effectively manage potential money laundering and terrorist financing risks.

You have to consider the nature and business of your clients and their relationships with you to determine the level of risk of money laundering and terrorist financing. In other words, you have to know your clients to perform a risk assessment. Knowing your clients is not limited to identification or record keeping requirements. It is about understanding your clients, including their activities, transaction patterns, how they operate and so on. Other elements, such as the

magnitude of a client's assets or the number of transactions involved, might also be relevant. Although you should obtain this information through your dealings with the client, it does not necessarily mean that you have to ask the client for additional information or identification documents. You should consider clients you do not know as higher-risk than those that you know.

Clients within business relationships

You enter into a business relationship when a client opens an account or undertakes two or more transactions with you that require you to ascertain the identity of the client, regardless of whether the transactions are related to each other. You have to assess the client risk in both new and existing business relationships.

You have to perform a risk assessment at the beginning of a business relationship, although a comprehensive risk profile of the relationship may only become evident once you perform ongoing monitoring of those clients. However, even at the beginning of new business relationships, the client identification and information gathering measures should be robust enough to provide the information needed to feed into your risk assessment. The risk assessment requires you to consider each one of your clients when assessing their risk for money laundering and terrorist activity financing. However, an individual written assessment is not required for each client, so long as you can demonstrate that you put your client in the correct risk category, according to your policies and procedures, and risk assessment.

When assessing the risk of a business relationship, consider the relationship's duration, its activities, the number of accounts (if applicable), and the products and services used. You may also consider third parties that can be involved in the business relationship for their impact on the relationship's risk if you are required to make third party determination. Furthermore, you also have to consider the beneficial owners of an entity for their impact on risk, if you are required to obtain this information. See Guideline 6 for your sector for more information about third party determinations and beneficial ownership information requirements.

Situations where you conduct a transaction for which a client is acting on behalf of a third party but does not know anything about the third party may lead you to consider that client as a high risk. Similarly, you must consider as a high risk a client acting on behalf of an entity when the client is not aware of the entity's beneficial owners (such as the names of the entity's directors or the individuals controlling the entity, for example).

If you are required to determine that your client is a politically exposed foreign person, and determine that he or she is a politically exposed foreign person, you must consider that client as a high risk. See the definition of a politically exposed foreign person in Guideline 6.

If as a result of your ongoing monitoring you consider that the risk of a money laundering or a terrorist financing offence in a business relationship is high, your risk assessment in your compliance regime must treat that client as a high risk. In such a case, you must conduct more frequent monitoring of your business relationship with that client, update that client's identification information more frequently, and adopt any other appropriate enhanced measures (examples of measures can be found in subsection 6.4).

You should also consider unusual circumstances, cash-intensive businesses and other indicators as potential high risks.

Clients outside of business relationships
Where your dealings with a client are limited to a single transaction, the client does not have an account, and the client is not opening an account, this is **not** considered to be a business relationship. However, you still need to complete a risk assessment of that client. As well, if you suspect that the transaction is related to a money laundering or terrorist financing offence, you have to report it to FINTRAC as explained in *Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC*.

6.2 Risk mitigation

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.

6.2.1 Measures to mitigate the risks

You have to include risk mitigation measures in your written policies and procedures. The following summarizes different types of mitigating measures you could develop and apply through your compliance policies and procedures.

In all situations, you should consider internal controls such as:

- focussing on your operations (products and services, clients and business relationships, geographic locations, and any other relevant factors) that are more vulnerable to abuse by money launderers and criminals;
- informing senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious transaction reports filed;
- providing for program continuity despite changes in management, employees or structure;

- focussing on meeting all regulatory record keeping and reporting requirements, recommendations for anti-money laundering and anti-terrorist financing compliance and providing for timely updates in response to changes in requirements;
- enabling the timely identification of reportable transactions and ensure accurate filing of required reports;
- incorporating anti-money laundering and anti-terrorist financing compliance into job descriptions and performance evaluations of appropriate personnel; and
- providing for adequate supervision of employees that handle currency transactions, complete reports, monitor for suspicious transactions, or engage in any other activity that forms part of your anti-money laundering and anti-terrorist financing program.

Here are examples of measures you may undertake to mitigate your risk:

- increasing your awareness of high risk situations within business lines across your entity;
- increasing the frequency of ongoing monitoring of transactions or business relationships ;
- escalating the approval of the establishment of an account or relationship even if you are not otherwise required to do so (see additional requirements for certain sectors in subsection 6.5);
- increasing the levels of ongoing controls and reviews of relationships; and
- reviewing your own internal controls, to ensure that you have:
    - personnel that have clear lines of authority, responsibility and accountability;
    - adequate segregation of duties (for example, an employee opening an account for a client is not authorized to also approve its opening as that authorization is the responsibility of someone else in the organization);
    - proper procedures for authorization (for example, an employee processing a transaction for which the amount exceeds a certain threshold has to follow a procedure to get approval for the transaction by someone else in the organization); and
    - internal reviews to validate the risk assessment processes.

You may also consider additional measures such as:

- seeking additional information beyond the minimum requirements to ascertain the client’s identity or the beneficial ownership information of an entity;
- requesting high-risk clients provide additional, documented information regarding controls they have implemented to safeguard their operations from abuse by money launderers and terrorists;
- getting independent verification of information (that is, from a credible source other than the client);

- stopping any transaction with a potential client until identification and account opening information has been obtained;
- implementing an appropriate process to approve all relationships identified as high-risk as part of the client acceptance process or declining to do business with potential clients because they exceed your risk tolerance level;
- implementing a process to exit from an existing high-risk relationship which management sees as exceeding your risk tolerance level.

If you are a financial entity, a securities dealer, a life insurance company, broker or independent agent, or a money services business, you have additional requirements related to risk mitigation. See subsection 6.5 for more information.

6.3 Keeping client identification, beneficial ownership and business relationship information up to date

You have to develop and apply policies and procedures to keep client identification information up to date. If you are a financial entity, a securities dealer, a life insurance company, broker or agent, or a money services business, your ongoing monitoring obligations also require you to keep beneficial ownership information up to date. All sectors must develop and apply policies and procedures to keep information on business relationships up to date. When you identify a client as high-risk, you must conduct more frequent ongoing monitoring and updating of client identification information, as well as any other appropriate enhanced measures (examples of these measures can be found in subsection 6.4). However, dealers in precious metals and stones only need to perform enhanced monitoring of business relationships they consider to be high-risk.

Client identification information
Client identification information depends on the information you have to confirm or obtain from your clients and the records you have to keep. Client identification information that is required to be updated generally includes:

- For an **individual**, the individual's name, address, telephone number and occupation or principal business.
- For a **corporation**, its name and address and the names of the corporation's directors.
- For an **entity other than a corporation**, its name, address and principal place of business.

Measures to keep client identification up to date include asking the client to provide information to confirm or update their identification information.

In the case of an individual client, measures can also include confirming or updating the information through the options available to ascertain the identity of individuals who are not physically present.

In the case of clients that are entities, measures to keep client identification up to date include consulting a paper or an electronic document to confirm information or obtaining the information verbally from the client.

Keeping client identification information up to date is part of your ongoing monitoring obligations. The frequency with which you review client identification information and keep it up to date will vary depending on your risk assessment of your client.

Information on beneficial ownership and control

If you are a financial entity, a securities dealer, a life insurance company, broker or independent agent, or a money services business, you have to obtain, take reasonable measures to confirm, and keep records of the information about an entity's beneficial ownership. Beneficial ownership refers to the identity of the individuals who ultimately control the corporation or entity, and cannot be another corporation or another entity. You must search through as many levels of information as necessary in order to determine beneficial ownership. However, there may be cases where there is no individual who owns or controls 25% or more of an entity. You must still keep a record of the measures you took and the information you obtained in order to reach that conclusion.

Here is a short, non-exhaustive list of documents that could be provided by clients to confirm beneficial ownership information:

In the case of corporations:

- Articles of incorporation
- Annual returns
- Shareholder agreements

In the case of entities other than corporations:

- Articles of constitution
- Partnership agreements
- Records of decisions

Beneficial ownership information is:

- for a corporation:
    - the names of all its directors;
    - the names and addresses of all individuals who directly or indirectly own or control 25% or more of the corporation's shares; and
    - information on the ownership, control, and structure of the corporation.

The following is an example of ownership, control and structure of a corporation: ABC Canada Inc. is a for-profit corporation with 100 privately traded shares in circulation. It is incorporated pursuant to the Canada Business Corporation Act. John Brown owns 15 of the shares and Green Company Ltd. owns the remaining

85 shares. James Smith is President of ABC's board of directors; his wife, Jane Smith, is ABC's Chief Financial Officer; and their three children make up the other members of the board.

In this example:

- *Ownership of the corporation is shared by John Brown (15 % of the shares) and Green Company Ltd. (85% of the shares);*
- *All members of the board of directors (the 5 members of the Smith family) exercise control of the corporation. Because Green Company Ltd. owns 85% of the corporation's shares, it also exercises control. However, in a case like this, you must research further into the ownership until you find an individual who owns enough shares in Green Company to own or control 25% or more of ABC Canada or until you find that there is no such individual;*
- *The structure of the corporation is that of a privately traded, for-profit corporation incorporated pursuant to the Canada Business Corporation Act.*

- for a trust:
  - the names and addresses of all trustees and all known beneficiaries and settlors of the trust; and
  - information on the control and structure of the trust.

The trust deed will provide you the information on the control and structure of the trust. If you are unable to obtain the names and addresses of the trustees, beneficiaries or settlors of the trust, you must find the name of the senior managing officer of the trust, that is, the person in the trust company who is in fact responsible for the management of that trust, such as an account manager.

- for an entity that is other than a corporation or trust:
  - the names and addresses of all individuals who directly or indirectly own or control 25% or more of the entity; and
  - information on the ownership, control, and structure of the entity.

The following is an example of ownership, control and structure of an entity that is neither a corporation nor a trust:

Rainbow Money Services is a money services business (MSB) in Vancouver owned by Howard and Betty. Howard and Betty paid a lawyer to draft a partnership agreement for the business, which they both signed. According to the agreement, Howard will invest $100,000 in the partnership to buy equipment and rent space for the MSB, and Betty will be solely responsible for operating the MSB and performing its business. All decisions related to the partnership must be unanimous; in case of a disagreement, either partner can decide to end the partnership. Howard and Betty will split the income from the MSB 50/50, and if

they decide to end the partnership, Howard will get 85% of the proceeds of the sale of the business assets, while Betty will get 15%.

In this example:

- *Ownership of the entity is shared between Howard and Betty;*
- *Howard and Betty both control the partnership;*
- *The structure of the entity is a partnership between Howard and Betty, constituted pursuant to a contract governed by the laws of British Columbia.*

If this information cannot be obtained or its accuracy cannot be confirmed, you have to:

- obtain the name of the most senior managing officer of the corporation, trust or other entity;
- take reasonable measures to ascertain the identity of the most senior managing officer of the corporation, trust or other entity; and
- treat that corporation, trust or other entity as high-risk in your risk assessment document of your compliance regime.

You do not need to ascertain the identity of the most senior managing officer when there is no individual who owns or controls 25% or more of an entity.

In the context of this section, the senior managing officer of a corporation or an entity may include but is not limited to its director, chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, as well as any individual who performs any of those functions. It also includes any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer. In the case of a sole proprietor or a partnership, the senior managing officer can be the owner or the partner.

In the context of this section, the senior managing officer of a trust is the trustee, that is, the person who is authorized to administer or execute on that trust.

To ascertain the identity of the most senior managing officer, use one of the methods described in section 4 (under “How to ascertain the identity of an individual”) of *Guideline 6: Record Keeping and Client Identification*, or obtain it through public sources. You also have to keep a record of this information.

If you have to confirm the existence of an entity that is a not-for-profit organization, you also have to do the following:

- Determine whether or not that entity is a registered charity for income tax purposes and keep a record to that effect. To make this determination, you can ask the client or consult the charities listing on the Canada Revenue Agency website (http://www.cra-arc.gc.ca).

- If that entity is not a registered charity, determine whether or not it solicits charitable financial donations from the public and keep a record to that effect. To make this determination, you can ask the client.

Keeping beneficial ownership information up to date is part of your ongoing monitoring obligations. The frequency with which you review beneficial ownership information and keep it up to date will vary depending on your risk assessment of your client.

Exceptions to obtaining information on beneficial ownership and control

The requirement to confirm the existence of a corporation, trust or other entity at the opening of an account does not apply to a group plan account held within a dividend or a distribution reinvestment plan if the sponsor of the plan is an entity that trades shares or units on a Canadian stock exchange and operates in a country that is a member of the Financial Action Task Force.

If you deal in reinsurance, the beneficial ownership requirements do not apply to you regarding those dealings.

Business relationship information

A business relationship is a relationship that you establish with a client to conduct financial transactions or provide services related to those transactions. A business relationship can be established within or outside of an account.

Account-based business relationships: You are in a business relationship with a client that holds an account with you. You enter into a business relationship when a client opens an account with you. For a new or existing client that has one or more accounts, it includes all transactions and activities relating to those accounts.

Non-account-based business relationships: If your client does not have an account, you enter into a business relationship when you conduct two or more transactions in which you have to:

- ascertain the identity of the individual; or
- confirm the existence of a corporation or other entity.

In such a case, the business relationship only includes transactions and related activities for which you have to ascertain the identity of your client.

You should determine that a business relationship has been established as soon as reasonably practicable following the second transaction requiring that the client's identity be ascertained. As a best practice, this should be done within 30 calendar days.

A business relationship is established when two transactions that require you to ascertain the identity of your client occur within a maximum of five years from one another. If a period of five years passes from the last transaction that required you to ascertain the identity of your client, the business relationship with that client ceases in the case of non-account-based business relationships. In the case of clients who hold an account, the business relationship ceases five years after the client closes that account.

When you enter into a business relationship with a client, you have to keep a record of the purpose and intended nature of the business relationship. You also have to review this information on a periodic basis and keep it up to date. This is done to ensure that you continue to understand your client's activities over time so that any changes can be measured to detect high risk, thus increasing the frequency of ongoing monitoring, updating of client identification information, and any other appropriate enhanced measures (examples of these measures can be found in subsection 6.4).

The frequency with which business relationship information is to be kept up to date will vary depending on your risk assessment of your client. You should monitor business relationships you consider high-risk more frequently.

6.4 Ongoing monitoring of business relationships

As part of the ongoing monitoring requirements of your compliance regime, all sectors must develop and apply policies and procedures to keep information on business relationships up to date. When you identify a client as high-risk, you must conduct more frequent ongoing monitoring and updating of client identification information, as well as any other appropriate enhanced measures. However, dealers in precious metals and stones only need to perform enhanced monitoring of business relationships they consider to be high-risk.

Here is a non-exhaustive list of enhanced measures you could take to mitigate the risk in cases of high-risk business relationships:

- Obtaining additional information on the client (e.g. occupation, volume of assets, information available through public databases, Internet, etc.).
- Obtaining information on the source of funds or source of wealth of the client.
- Obtaining information on the reasons for intended or conducted transactions.
- Obtaining the approval of senior management to enter into or maintain the business relationship.
- Identifying patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the client's name with a bank subject to similar client due diligence standards.
- Increased monitoring of transactions of higher-risk products, services and channels.

- Establishing more stringent thresholds for ascertaining identification.
- Gathering additional documents, data or information; or taking additional steps to verify the documents obtained.
- Establishing transaction limits.
- Increasing awareness of high-risk activities and transactions.
- Increasing internal controls of high-risk business relationships.
- Obtaining the approval of senior management at the transaction level for products and services that are new for that client.

Ongoing monitoring means that you have to monitor your business relationship with a client on a periodic basis. The risk assessment requires you to consider each one of your clients when assessing their risk for money-laundering and terrorist activities financing. However, an individual written assessment is not required for each client, so long as you can demonstrate that you put your client in the correct risk category, according to your policies and procedures, and risk assessment. Use the risk assessment that applies to the business relationship with a client in your compliance regime to:

- detect suspicious transactions that have to be reported;
- keep client identification, the purpose and intended nature of the business relationship, and (when required) beneficial ownership information up to date;
- reassess the level of risk associated with the client's transactions and activities; and
- determine whether the transactions or activities are consistent with the information previously obtained about the client, including the risk assessment of the client.

The above-listed requirements do not need to follow the same timeframe, so long as you monitor your high-risk clients more frequently and with more scrutiny than you do your low-risk clients.

In the context of monitoring on a periodic basis, your monitoring will vary depending on your risk assessment of the client. As part of your ongoing monitoring obligations, you have to monitor all of your business relationships, and you must monitor business relationships you consider high-risk more frequently.

If as a result of your ongoing monitoring you consider that the risk of a money laundering or a terrorist financing offence in a business relationship is high, your risk assessment in your compliance regime should treat that client as a high risk. In this case, you must conduct more frequent monitoring of your business relationship with that client, update their client identification information more frequently, and adopt any other appropriate enhanced monitoring measures (examples of measures can be found above).

You could consider the following measures to monitor high-risk situations:

- review transactions based on an approved schedule that involves management sign-off;
- develop reports or perform more frequent review of reports that list high-risk transactions. Flag activities or changes in activities from your expectations and elevate concerns as necessary;
- set business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;
- review transactions more frequently against suspicious transaction indicators relevant to the relationship. See *Guideline 2: Suspicious Transactions* for more information about indicators.

If you are a financial entity or a securities dealer, you have additional requirements related to ongoing monitoring. See subsection 6.5 for more information.

6.5 High-risk situations for certain sectors

In addition to the risk-based approach process described in subsections 6.1 to 6.4, certain sectors have further requirements. These are described below, by sector.

6.5.1 Financial entities

Ongoing monitoring for correspondent banking relationships

A correspondent banking relationship is one created by an agreement or arrangement between a foreign financial institution and a financial entity (as described in section 2.1). It only applies to an agreement where the financial entity is to provide services, such as international electronic funds transfers, cash management and cheque clearing, to the foreign financial institution. If the agreement were only for the foreign financial institution to provide services to the financial entity, then it would not be considered a correspondent banking relationship for these purposes.

When you enter into a correspondent banking relationship with a foreign financial institution, you have to take reasonable measures to find out whether the foreign financial institution has anti-money laundering and anti-terrorist financing policies and procedures in place, including procedures for the approval of opening new accounts. In this context, reasonable measures include asking the foreign financial institution for the information about their policies and procedures. If it does not have such policies and procedures in place, you have to take reasonable measures to conduct ongoing monitoring of all transactions (as explained in subsection 6.4) within the correspondent banking relationship to detect suspicious transactions.

You could also consider monitoring transactions that you have flagged as questionable in the context of correspondent banking relationships, such as the following:

- large value or large volume transactions that involve numbered monetary instruments (for example travellers' cheques, money orders or bank drafts);
- transactions that appear unusual in the context of the relationship; or
- transactions that appear to be structured to avoid your monitoring system.

In addition, you have to take reasonable measures to find out, based on publicly available information, whether there are any civil or criminal sanctions imposed against the foreign financial institution in respect of anti-money laundering or anti-terrorist financing requirements. If there are any sanctions, the correspondent banking relationship is considered a high risk. In that case, you have to take reasonable measures to conduct ongoing monitoring of all transactions within the correspondent banking relationship to detect suspicious transactions. To do so, consider the measures described above as well as those in subsection 6.4.

6.5.2 Financial entities and securities dealers

Politically exposed foreign persons determination for existing and new account holders

If you are a financial entity or a securities dealer, your risk assessment must identify high-risk situations for money laundering and terrorist financing where existing account holders (including credit card accounts opened by financial entities) might be politically exposed foreign persons. This means that your policies and procedures have to include reasonable measures to determine whether or not an existing account holder that is considered high risk is a politically exposed foreign person. You also have to take reasonable measures to determine whether or not a new account holder is a politically exposed foreign person. Whether for a new or an existing account, reasonable measures could include the automated review of your individual client base using commercial software or publicly available information about politically exposed foreign persons. You could also ask your clients.

Once you have determined that an account holder is a politically exposed foreign person, you have additional requirements. They include establishing the source of funds and getting senior management approval to keep an account open (whether for a new or an existing account). You also have to conduct ongoing monitoring of transactions related to the account to detect suspicious transactions. See Guideline 6 for your sector for more information about politically exposed foreign persons.

6.5.3 Financial entities, life insurance companies, brokers or agents, or money services businesses

Politically exposed foreign persons determination for certain transactions

If you are a financial entity, a life insurance company, broker or agent, or a money services business, you have additional requirements for certain types of transactions of $100,000 or more. You have to determine if you are dealing with a politically exposed foreign person. If so, you have to establish the source of funds and get senior management to review the transaction. See Guideline 6 for your sector for more information about politically exposed foreign persons.

7 Ongoing Compliance Training

If you have employees, agents or other individuals authorized to act on your behalf, your compliance regime has to include training. This is to make sure that all those who have contact with clients, who see client transaction activity, who handle cash or funds in any way or who are responsible for implementing or overseeing the compliance regime understand the reporting, client identification and record keeping requirements. This includes those at the “front line” as well as senior management.

If you are a sole proprietor (not a corporation) with no employees, agents or other individuals authorized to act on your behalf, you are not required to have a training program in place for yourself. However, your policies and procedures must be in place, updated and will have to be reviewed every two years to test their effectiveness.

Your training program has to be in writing and you have to maintain it. This means that the program itself has to be in writing, but the way the training is delivered does not have to be in writing. For example, you could deliver your training program using computer-based software, information sessions, face-to-face meetings, etc. You also have to ensure that your training program is reviewed and adjusted in a timely manner to reflect your needs.

In addition, others who have responsibilities under your compliance regime, such as information technology and other staff responsible for designing and implementing electronic or manual internal controls, should receive training. This could also include the appointed compliance officer and internal auditors.

Standards for the frequency and method of training, such as formal, on-the-job or external, should be addressed. New people should be trained before they begin to deal with clients. All should be periodically informed of any changes in anti-money laundering or anti-terrorism legislation, policies and procedures, as well as current developments and changes in money laundering or terrorist activity financing schemes particular to their jobs. Those who change jobs within your organization should be given training as necessary to be up-to-date with the policies, procedures and risks of exposure to money laundering or terrorist financing that are associated with their new job.

The method of training may vary greatly depending on the size of your business and the complexity of the subject matter. The training program for a small business may be less sophisticated.

When assessing your training needs, consider the following elements:

- **Requirements and related liabilities**
  The training should give those who need it an understanding of the reporting, client identification and record keeping requirements as well as penalties for

not meeting those requirements. For more information about this, see the other guidelines regarding each of those requirements applicable to you.

- **Policies and procedures**
  The training should make your employees, agents, or others who act on your behalf aware of the internal policies and procedures for deterring and detecting money laundering and terrorist financing that are associated with their jobs. It should also give each one a clear understanding of his or her responsibilities under these policies and procedures.

  They need to understand how their institution, organization or profession is vulnerable to abuse by criminals laundering the proceeds of crime or by terrorists financing their activities. Training should include examples of how your particular type of organization could be used to launder illicit funds or fund terrorist activity. This should help them to identify suspicious transactions and should give you some assurance that your services are not being abused for the purposes of money laundering or terrorist financing.

  Employees should also be made aware that they cannot disclose that they have made a suspicious transaction report, or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether it has started or not. They should also understand that no criminal or civil proceedings may be brought against them for making a report in good faith.

- **Background information on money laundering and terrorist financing**
  Any training program should include some background information on money laundering so everyone who needs to can understand what money laundering is, why criminals choose to launder money and how the process usually works. They also need to understand what terrorist financing is and how that process usually works. For more information about this, see *Guideline 1: Backgrounder* and FINTRAC's website (http://www.fintrac-canafe.gc.ca).

All businesses should consult, if possible, training material available through their associations. In addition, FINTRAC makes material available on its website that can provide help with training. For example, a practice environment is available within F2R, FINTRAC's Web-based tool for electronic reporting, that can be used for training. You can use this to complete simulated electronic reports. However, as a reporting entity described in section 2, you are responsible to have your own training program and to ensure that each component of the program is reviewed and adjusted to meet your needs.

8 Review Every Two Years

Another component of a comprehensive compliance regime is a review of your compliance policies and procedures to test their effectiveness. The review has to be done every two years. It has to cover your policies and procedures, your

assessment of your business' risks related to money laundering and terrorist financing, and your training program to test their effectiveness. The review of your assessment of risks related to money laundering and terrorist financing has to cover all the components of the risk-based approach as explained in subsections 6.1 to 6.5, including your policies and procedures on risk assessment, risk mitigation and ongoing monitoring. The ongoing monitoring of your clients should inform your review of your compliance regime in terms of the effectiveness of your risk assessment. This will help evaluate the need to modify existing policies and procedures or to implement new ones. This may also lead you to update your compliance policies and procedures.

If you are in a sector that is regulated at the federal or provincial level, the need for review of your compliance policies and procedures could also be triggered by requirements administered by your regulator.

The review is to be conducted by an internal or external auditor, if you have one. The review by an internal or external auditor could include interviews, tests and samplings, such as the following:

- interviews with those handling transactions and with their supervisors to determine their knowledge of the legislative requirements and your policies and procedures.
- a review of the criteria and processes for identifying and reporting suspicious transactions.
- a sampling of large cash transactions followed by a review of the reporting of such transactions.
- a sampling of international electronic funds transfers (if those are reportable by the reporting entity in question) followed by a review of the reporting of such transactions.
- a sampling of clients to see if the risk assessment was adequate.
- a sampling of clients to see if the frequency of ongoing monitoring is adequate.
- a sampling of high-risk clients to review the enhanced measures taken.
- a test of the validity and reasonableness of any exceptions to large cash transaction reports including the required annual report to FINTRAC (this is applicable only for financial entities who choose the alternative to large cash transactions for certain business clients).
- a test of the record keeping system for compliance with the legislation.
- a test of the client identification procedures for compliance with the legislation.
- a review of the risk assessment.

The scope of the review has to be documented. The scope and details of the review will depend on the nature, size and complexity of your operations. The review process should be well documented and should identify and note weaknesses in policies and procedures. The results of the review also have to be documented, along with corrective measures and follow-up actions.

Reporting to senior management
If you are an entity, within 30 days of the review, you have to report the following in writing to one of your senior officers:

- the findings of the above review;
- any updates that were made to the policies and procedures during the review period;
- the status of implementation of the policies and procedures updates.

Any deficiencies should be identified and reported to senior management or the board of directors. This should also include a request for a response indicating corrective actions and a timeline for implementing such actions.

Self-review
If you do not have an internal or external auditor, you can do a "self-review." If feasible, this self-review should be conducted by an individual who is independent of the reporting, record keeping and compliance-monitoring functions. This could be an employee or an outside consultant. The objective of a self-review is similar to the objectives of a review conducted by internal or external auditors. It should address whether policies and procedures are in place and are being adhered to, and whether procedures and practices comply with legislative and regulatory requirements.

9 FINTRAC's Approach to Compliance Monitoring

FINTRAC has a responsibility to ensure compliance with your legislative requirements under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. To do this, FINTRAC can examine your compliance regime and records. FINTRAC may also periodically provide you with feedback about the adequacy, completeness and timeliness of the information you have reported.

FINTRAC favours a co-operative approach to compliance monitoring. The emphasis will be on working with you to achieve compliance. When compliance issues are identified, FINTRAC intends to work with you in a constructive manner to find reasonable solutions. If this is not successful, FINTRAC has the authority to disclose information related to non-compliance cases to the appropriate law enforcement agencies. FINTRAC also has the authority to impose administrative monetary penalties (AMPs) in instances of non-compliance. Penalties for non-compliance are described in more detail in section 10.

FINTRAC's compliance program uses risk management strategies to identify those most in need of improving compliance. Efforts will be focused on areas where there is greater risk of non-compliance and in which the failure to comply could have significant impact on the ability to detect and deter money laundering and terrorist financing.

Finally, FINTRAC works with other regulators at the federal and provincial levels to identify areas of common interest and address the potential for overlap in some areas of its responsibilities. In that context, FINTRAC continues to explore avenues for cost efficiencies, consistency of approach and information sharing. Regulators may share information with FINTRAC when they have an agreement to do so.

10 Penalties for Non-Compliance

Failure to comply with your legislative requirements can lead to criminal charges against you **if you are a reporting entity described in section 2**. The following are some of the penalties:

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

Failure to comply with your legislative requirements can lead to the following administrative monetary penalties (AMPs) against you if you are a reporting entity described in section 2:

- failure to implement any of the five elements of the compliance regime described in section 3 could lead to an administrative monetary penalty of up to $100,000 for each one.
- failure by an entity to report the required information to senior management within 30 days after the review of its compliance program could lead to an administrative monetary penalty of up to $100,000.
- failure to ascertain the identity of clients, keep records, monitor financial transactions and take mitigating measures in situations where risk of money laundering or terrorist financing is high could lead to an administrative monetary penalty of up to $100,000.

For more information on penalties, you can also consult the “Penalties for non-compliance” section of FINTRAC's website.

11 Comments?

These guidelines will be reviewed on a periodic basis. If you have any comments or suggestions to help improve them, please send your comments to the mailing address provided below, or by email to guidelines-lignesdirectrices@fintrac-canafe.gc.ca.

12 How to Contact FINTRAC

For further information on FINTRAC and its activities, reporting and other obligations, please go to FINTRAC's website (http://www.fintrac-canafe.gc.ca) or contact FINTRAC:

Financial Transactions and Reports Analysis Centre of Canada
234 Laurier Avenue West, 24th floor
Ottawa ON K1P 1H7
Canada

Toll-free: 1-866-346-8722