IIROC OCRCVM

Investment Industry Regulatory Organization of Canada

Organisme canadien de réglementation du commerce des valeurs mobilières

Anti-Money Laundering Compliance Guidance

October 2010

Table of Contents

1. Introduction

1.1 Purpose and Scope

This notice provides guidance on compliance with the anti-money laundering (AML) and countering the financing of terrorism (CFT) requirements applicable to IIROC Dealer Members. It replaces and updates the IDA brochure *"Deterring Money Laundering Activity."*

Securities firms have been subject to federal statutory and regulatory requirements regarding client identification since 1993. The requirements were expanded in 2001/2 and again in 2008 and are supplemented by IIROC rules directed at preventing both money laundering and market abuse.

The 2008 amendments included several significant changes, such as

- The requirement to conduct an AML risk assessment, which requires an understanding of money laundering and terrorist financing risks and techniques;
- The identification of politically exposed foreign persons and implementation of special procedures for their accounts; and
- Increased identity verification procedures for non face-to-face clients.

This guidance can only provide a high level outline of the expectations on Dealer Members, along with pointers to other resources that will assist those needing to go beyond the available guidance. It also assumes that many of the existing practices currently employed within the industry to deter money laundering will continue. For example, most Dealer Members do not accept cash deposits or limit them to amounts

well below the threshold for large cash transaction reporting. Therefore this document will not provide guidance on controls related to large cash deposits.[1]

Given the variety and complexity of the securities industry today, the varying products and businesses that can be housed within a single firm, the considerable differences among and within securities firms and the new requirements for firm-specific risk- and self-assessments, no one standard or model program can be appropriate for all firms. This guide should help a Dealer Member adapt its AML/CFT compliance program to the firm's business: the breadth and scope of its customer base, type of accounts and transactions, extent of international activities, differing natures and risks of its lines of business and other relevant factors.

1.2 Marketplace Members

The AML/CFT requirements are applicable to "persons and entities 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." Because alternative trading systems ("ATSs") are both marketplaces and Dealer Members, the requirements are applicable to them, i.e. ATSs are required to have a compliance program including anti-money laundering policies and procedures, risk assessment and audits .

However, in practice there may be few regulations that have practical application to an ATS. If the ATS provides only quotation and trade execution services to subscribers, it may never open an account for dealing in securities and will never have to identify customers and verify their identities. If an ATS does have customer accounts, they may only be for other dealers or institutions that are exempt from customer due diligence and identity verification requirements.

[1] This is not to say that such policies can be ignored in a Dealer Member's self-policing. For example, it should be a standard item in the audit of a business location that handles client funds to spot-check bank deposits to assure that the business location complies with limits on cash deposits. In this regard, it is useful to note that in 2004 the Bank of Ireland was fined £375,000 by the Financial Services Authority for failing to detect a series of suspicious cash transactions in a business location.

This guidance is therefore focused on more traditional Dealer Members.

2. Background – Money Laundering Under the Criminal Code

Offences regarding the possession of and dealings in the proceeds of crime, money laundering and the financing of terrorism are established in the *Criminal Code* (RSC 1985, c. C-46).

2.1 Possession and Money Laundering Offences

It is an offence under section 354(1) of the *Criminal Code* to possess any property or the proceeds of any property knowing that all or part of it was obtained by or derived directly or indirectly from the commission in Canada of an indictable offence or an act or omission anywhere that would have been an indictable offence in Canada.

Money laundering itself comes under Section 462.31 of the *Criminal Code*, which makes it an offence to use, transfer the possession of, send or deliver, transport, transmit, alter, dispose of or otherwise deal with any property or the proceeds of property with intent to conceal or convert the property, knowing or believing that all or a part of the property was obtained directly or indirectly by the commission of a "designated offence." Again the section covers the proceeds of both designated offences committed in Canada and those committed outside of Canada that would have been designated offences if committed in Canada.

A designated offence, often called a "predicate offence," is defined in section 462.3(1) of the *Criminal Code* as any indictable offence under any Act of Parliament other than offences established by regulation. Conspiracy, counseling, or attempting to commit or being an accessory after the fact to an indictable offence is also a designated offence.

Designated offences of particular interest to Dealer Members include:

- Offences relevant to the securities markets:
    - breach of trust;
    - fraud;
    - stock market manipulation;
    - insider trading; and
    - money laundering itself;
- Terrorism and the financing of terrorism because of special customer due diligence and reporting requirements under various regulations described below; and
- Bribery and corruption because of the provisions regarding secret commissions and the PCMLTFA requirements regarding politically exposed foreign persons described in this guidance.

However, Dealer Members should be cognizant of the wide variety of designated offences, which extends beyond *Criminal Code* offences to include, for example:

- Possession of or trafficking in scheduled substances under the *Controlled Drugs and Substances Act* (RSC 1996, C. 19);
- Deceptive telemarketing contrary to s. 52.(1) of the *Competition Act* (RSC, 1985, c. C-34);
- Smuggling and evasion of duties contrary to s. 153 or 159 of the *Customs Act* (RSC 1985, c. 1 (2nd Supp)); and
- Unlawful manufacture, packaging, stamping or sale of tobacco and tobacco products contrary to s. 25, 27, 29 or 32.1(1) of the *Excise Act, 2001* (2002, C. 22).

Other designated offences include a broad variety of criminal conduct such as weapons offences, counterfeiting, forgery, uttering, gambling, charging a criminal interest rate, offences related to prostitution, possession or publication of obscene material or child pornography, participation in a criminal organization, extortion, arson and murder.

2.2 Penalties for Possession of the Proceeds of Crime

The maximum punishment under the *Criminal Code* for possession of proceeds of crime greater than $5,000 is ten years imprisonment. If the proceeds are $5,000 or less, a possession prosecution can be by indictment, in which case the maximum penalty is two years imprisonment.

The maximum penalty for a money laundering conviction is 10 years imprisonment, whatever the amount laundered.

Possession of less than $5,000 of the proceeds of a crime or laundering in any amount can also be prosecuted by summary conviction, in which case the maximum penalty is six months imprisonment or a $5,000 fine or both. Default of a summary conviction fine can result in up to six months imprisonment.

2.3 Terrorist Property and Financing

Knowingly dealing, facilitating transactions or providing financial services in respect of terrorist property is an offence under s. 83.08(1) of the *Criminal Code* punishable by a maximum of 10 years imprisonment if convicted on indictment, or a $100,000 fine or up to one year imprisonment or both on summary conviction.

3. Background – PCMLTFA Requirements Applicable to Dealer Members

This section deals with the law and regulations requiring financial institutions, including securities dealers, to implement AML/CFT regimes, report certain transactions and maintain records.

3.1 The Proceeds of Crime (Money Laundering) and Terrorist Financing Act

The requirements for financial institutions to implement anti-money laundering mechanisms are based in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (RSC 2000, c. 17) (PCMLTFA). PCMLTFA is also the enabling legislation for the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

3.2 Regulations

Most of the specific AML/CFT requirements are contained in regulations under PCMLTFA. The four regulations applicable to Dealer Members are:

- The *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* [SOR/2002-184] (PCMLTF Regulations), which govern cash transaction reporting, customer due diligence, compliance and recordkeeping;
- The *Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations* [SOR/2002-184] (STR Regulations), which establish the format for the reporting of suspicious transactions, both completed and attempted;
- The *Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Penalties Regulations* [SOR/2007-292] (Administrative Penalty Regulations), which set out the procedures under which FINTRAC can impose administrative penalties for failure to comply with PCMLTFA or the regulations; and

- The *Cross-border Currency and Monetary Instruments Reporting Regulations* [SOR/2002-412] (Cross-border Regulations), which establish reporting requirements regarding cross-border movements of funds and monetary instruments including securities.

3.3 Offences and Penalties under PCMLTFA

Violations of particular requirements of PCMLTFA can be as high as a $2 million fine and five years imprisonment.

The penalties that can be imposed for violations of specific provisions of the requirements are shown in Appendix C.

3.4 Administrative Penalties

The Administrative Penalties Regulations, implemented at the end of 2008, give FINTRAC the authority to impose administrative sanctions on Dealer Members for violations of PCMLTFA and the regulations. A violation dealt with by an administrative penalty is not an offence under PCMLTFA. Use of the administrative penalty approach precludes a charge of violating PCMLTFA and vice versa.

Violations are classified as minor, serious or very serious. Maximum penalties are a $1,000 fine for a minor violation, a $100,000 fine for a serious violation and a $500,000 fine for a very serious violation. The violator's history of compliance with PCMLTFA and the regulations must be taken into account in establishing the penalty. The classification of violations most pertinent to Dealer Members is found in Appendix D.

FINTRAC can also offer to reduce the penalty by half if the violator enters into a compliance agreement with FINTRAC regarding the provision violated.

The process begins with a notice of violation setting out the violation and the proposed penalty. If the respondent does not respond to the notice by paying the proposed penalty or appealing the notice to the Director, the violation is deemed to have

occurred and FINTRAC will impose the penalty. On completion of all proceedings, FINTRAC can make violations public.

Sections 73.13 to 73.24 of PCMLTFA contain more detail on the procedures for imposition of administrative penalties.

4. Overview – Regulations

The most significant sections of PCMLTFA, the PCMLTF Regulations and IIROC Rules are shown in Appendix B.

IIROC has its own identification requirements, applicable to all IIROC Dealer Members. The IIROC identification requirements are set out in Dealer Member Rule 1300.1. The specific subsections are also shown in Appendix B.

4.1 IIROC Rules

The IIROC Rules which complement the AML/CFT requirements are intended to go beyond AML/CFT purposes, to assist in the proper policing of Canadian markets. Some of the IIROC customer due diligence rules require more information than the related PCMLTFA provisions in order to ensure that Dealer Members obtain customer information necessary for market regulators to investigate market abuse. Other provisions are less stringent.

The following examples illustrate the types of differences:

- The threshold for determining beneficial ownership of corporations and other entities is lower in IIROC Rules 1300.l (b) and (e) (10%) than in section 11.1(1) of the PCMLTF Regulations (25%);
- The IIROC Rules also contain a requirement to verify the identity of beneficial owners; and

- The IIROC Rules exempt certain types of institutions from the identification requirements such as when opening an account for a corporation or other entity that is or is an affiliate of a bank, trust company, securities dealer or similar financial institution subject to a satisfactory regulatory regime. The PCMLTF Regulations on identity verification do not provide for similar exemptions.

It is important to understand the differences and that in each case the more stringent rule applies.

4.2 Compliance Program Requirements

Section 9.6(1) of PCMLTFA requires dealers to establish an anti-money laundering compliance program, the specific details of which are established in section 71 of the PCMLTF Regulations, including:

- The appointment of a person to be responsible for the implementation of the program;
- The development and application of compliance policies and procedures that are kept up-to-date and approved by a senior officer;
- A program to assess the risk of a money laundering or terrorist financing offence being conducted through the firm;
- An ongoing compliance training program for employees[2] of the firm; and
- A review of the policies and procedures to test their effectiveness, to be conducted every two years by an internal or external auditor.

The risk assessment requirement was added in June, 2008. At the same time, the timing of a review was changed from "as often as necessary" to every two years.

[2] Where the term "employee" is used with reference to Dealer Members, it is inclusive of Registered Representatives in a principal/agent relationship with a Dealer Member and any employees of an agent that are engaged in the Dealer Member's business

5. Compliance Program Recommendations

5.1 Designation of an AML Compliance Officer

A firm must designate a Compliance Officer responsible for its anti-money laundering program (AML Officer). The AML Officer may effect his or her responsibilities through a specific department, unit, group or committee that, depending on the size, structure, business and resources of the firm, may be dedicated solely to the firm's anti-money laundering efforts, or may elect to have other responsibilities. The AML Officer, either directly or through the designated department, unit, group or committee, should be a central point of contact for communicating with FINTRAC and other agencies regarding issues related to the firm's anti-money laundering program.

Some financial services conglomerates have an enterprise AML/CFT department. A Dealer Member that is part of such a conglomerate must nonetheless designate a specific individual responsible for its AML program, but the person can be a member of or report to both the enterprise group and senior management of the Dealer Member. However, the Dealer Member remains responsible for its own AML/CFT program and cannot simply delegate everything to an enterprise group. Senior management of the Dealer Member must be kept informed of significant issues, and where the Regulations require approval of a senior officer it must be a senior officer of the Dealer Member.

5.2 Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT) Policy Statement

In addition to specific procedures, it is good practice for Dealer Members to adopt a broad statement that:

- Clearly sets forth the firm's policy against money laundering and any activity which facilitates money laundering or the funding of terrorist or criminal activities;

- Expresses the strong commitment of the firm and its senior management to comply with all laws and regulations designed to combat money laundering activity, including those rules and regulations requiring the reporting of transactions involving currency, certain monetary instruments, and suspicious activity;

- Emphasizes the responsibility of every employee to protect the firm from exploitation by money launderers;

- Sets forth the consequences of non-compliance with the applicable laws and firm policy, not only the significant criminal, civil and disciplinary penalties but also reputational harm that could ensue from any association with money laundering or terrorist financing;

- Includes references to specific procedures adopted by the firm to prevent and detect money laundering; and

- Affirms the Dealer Member's commitment to educating and training its employees in money laundering prevention.

The statement should be disseminated to all appropriate personnel, including those who deal directly with customers, supervisors and operations personnel who may effect client-directed non-trading transactions, using most effective method of distribution given the firm's structure. It should also be included in orientation packages for new employees or agents.

5.3 Risk Assessment

A Dealer Member must conduct a money laundering risk assessment of its business or businesses. Section 71 of the PCMLTF Regulations lists the factors to be taken into account in assessing risk as:

- clients and business relationships;

- products and delivery channels;
- geographic location of activities; and
- other relevant factors.

There are no universally accepted risk factors or risk scale. Each Dealer Member must look at its own operations and make its own determinations on higher or lower risk factors. These determinations should be based on the nature of money laundering and terrorist financing, but can also be inferred from the existing regulations. For example, the following could be taken as entailing higher AML/CFT risk, although it is not to be taken either as determinative or exhaustive:

- Customers:
    - Any vehicles such as corporations, offshore financial institutions or professionals acting as intermediaries that can be used to maintain the anonymity of principals;
    - Customers involved in the capital markets such as insiders, promoters, professional traders who are in a position or have motive to engage in market abuse;
    - Persons in positions subject to corruption, whether or not falling within the formal definition of "politically exposed foreign persons"; and
    - Customers involved in businesses more likely to be involved in illicit activity, such as cash-intensive businesses or import-export.
- Business relationships:
    - Customers that Dealer Member personnel do not meet face-to-face; and
    - Drop-in customers.

- Products and services:
    - Highly volatile products and markets such as commodity futures are frequently attractive to money launderers as providing an apparent source of extraordinary income or assets;
    - Highly volatile markets such as junior or less regulated marketplaces with thinly traded stocks are subject to manipulation and can therefore be used by money launderers both as a source of apparently legitimate profits and as a place to invest in criminal activity that can be highly profitable;
    - Physically portable products, particularly those of high value but low volume such as bearer bonds;
    - Deposit and withdrawal services; and
    - Wire transfer services.
- Delivery channels:
    - Those allowing off-shore access to assets and transactions; and
    - Those allowing anonymous access to assets and transactions, such as on-line systems, even if password-protected.
- Geographic location:
    - Business crossing jurisdictional boundaries;
    - High crime or highly corrupt jurisdictions;
    - Jurisdictions with weak AML/CFT controls; and
    - Tax havens and secrecy jurisdictions.

    (For additional information see Country Evaluations in Appendix G)

The risk analysis should be rigorous, but need not be complex. Firms having a high degree of homogeneity among clients or products can assess the relevant categories and then develop a set of unusual characteristics or indicators that might make a subset of clients or products higher risk.

A firm-wide risk assessment should begin with a determination of the factors relevant to the firm's business that will differentiate higher from lower risk businesses or customers. For example, some of the factors noted above will not be relevant to some Dealer Members because they do not deal in the relevant kinds of products, with particular types of customers or outside of the local jurisdiction.

Assessment processes often involve some kind of rating scale with factors to be taken into consideration in assigning a particular business, jurisdiction, client, etc. a higher or lower risk rating. The nature of the scale is not necessarily important; a low-medium-high scale can be just as useful as a 1 to 5 scale, although the latter is likely to be better when a multi-factor approach is used. What is critical is that those applying the scale understand the factors to be considered.

Risk assessment can be conducted across categories of customers, products or services first, but inter-relationships between these factors also have to be considered and assessed. For example, trading in a volatile, high risk market by an off-shore intermediary in a secrecy jurisdiction may present high AML/CFT risk where trading in the same market by a different type of customer or in a different product by the same intermediary may not.

A risk assessment process does not require that all customers be risk-assessed individually. While that might be appropriate in some circumstances, in others individual risk assessments may be restricted to those having a particular high-risk characteristic or engaging in higher risk activity.

Risk controls should be related to the source of the risk. For example, where the Dealer Member manages accounts on a discretionary basis, the nature of the securities

transactions is low risk because it is controlled by the dealer. In such a case any additional risk controls would be at the customer due diligence stage.

Extra monitoring or controls on a customer or type of business should relate directly to the source of the risk. Potential controls include:

- Higher levels of customer due diligence such as:
    - Increased due diligence when establishing a relationship. Increased due diligence can range from internet searches to hiring of due diligence professionals; and
    - More frequent reviews of customer information to ensure it is up-to-date.
- Higher levels of monitoring such as:
    - More frequent account reviews;
    - Non-transactional reviews such as reviews of account value; and
    - Special approval requirements for specific types of transactions.

The risk assessment program must be formally established, and records maintained of its application and the reasons behind its assessments. The assessments should be reviewed periodically or when there is a significant change to the firm's business affecting any of the major risk factors.

There are many sources of guidance available on risk factors and the risk in particular jurisdictions. Dealer Members may find the following reports to be useful: the MONEYVAL report: *"Use of securities in money laundering schemes"* and the Joint Money Laundering Steering Group Guidance *"Prevention of money laundering / combating the financing of terrorism"*, and Guidance for the UK Financial Sector *"Part II: Sectoral Guidance"* listed further reading at the end of this guidance.

5.4 Written Anti-Money Laundering Procedures

A firm's AML/CFT program must include procedures setting forth the systems and controls on which the firm relies, both to prevent and detect money laundering and to comply with the legislative and regulatory requirements and guidance issued by FINTRAC and others. The firm's written policies and procedures must cover:

- Customer due diligence, which is different from although very similar to "know-your-client" procedures;
- Procedures intended to protect the firm and its employees from inadvertently assisting in money laundering, such as those related to deposits of currency and cash equivalents;
- Procedures to monitor account activity for unusual or suspicious transactions or attempted suspicious transactions, investigate such transactions to determine whether they are suspicious and must be reported to FINTRAC, and report those that give reasonable grounds for suspicion; and
- Supplementary procedures implemented for those types of transactions or accounts deemed by the firm to pose a heightened risk for money laundering activity.

The policies and procedures should anticipate situations that may occur and direct employees on how to deal with them or who to consult. For example, there should be a procedure for deciding how to deal with a prospective customer who raises suspicions and or an existing customer who has engaged or is engaging in suspicious activity.

A Dealer Member's policies and procedures for compliance with other laws and regulations can be part of its AML/CFT program, but it is not sufficient to rely on systems and procedures designed to prevent fraud or supervise account activity to meet securities industry standards such as suitability.

AML/CFT policies and procedures may be developed separately, but they should ultimately be integrated with other compliance procedures. This will ensure that AML/CFT compliance reaches all aspects of the business and that AML/CFT procedures are not duplicative of procedures already undertaken for other purposes. While initial memoranda and other learning materials outlining specific AML/CFT procedures are a useful part of the educational process, integration into the firm's over-all KYC and supervisory procedures ensures that they become part of the established practice of all relevant personnel.

Similarly, information requirements related to AML/CFT regulations should be included in new account forms and related documents with sufficient information to ensure that the forms are properly completed. For example, a question regarding whether an applicant is a politically exposed foreign person should have a definition of the term, particularly if the form might be completed by the applicant.

In establishing AML/CFT procedures, conducting risk assessments and reviewing existing procedures, a firm should bring to bear a thorough understanding of money laundering risks arising from its types of business and clientele and of appropriate counter-measures. These change as money laundering and terrorist financing techniques adapt to preventive measures, as new products or services are developed and as new markets open. There is a wide variety of publicly available material, some of which is listed at the end of this guidance, to assist in risk assessments. Dealer Members can also keep up-to-date through attendance at industry seminars, discussions with industry and counterparts or by retaining outside experts.

Each Dealer Member's anti-money laundering procedures should be reviewed regularly and updated as necessary based on any legal/regulatory or business/operational changes, such as:

- Additions or amendments to existing anti-money laundering rules and regulations;

- Significant changes to the firm's business, such as new business lines, new types of customers or expansion into a new geographic areas; and

- Business process or technology changes affecting the way AML/CFT procedures are completed or records are stored.

The PCMLTF Regulations require that a Dealer Member's AML/CFT policies and procedures and any changes to them be approved by a "senior officer," who is defined in section 1.(1) as:

- A director who is a full-time employee;

- The CEO, COO, President, Secretary, Treasurer, Controller, CFO or any person who performs those functions; or

- Any other officer reporting directly to the Board, CEO or COO.

Based on the roles and responsibilities of the Chief Compliance Officer (CCO) set out in IIROC Dealer Member Rule 38 and the definition of an Executive as set out in Dealer Member Rule 1, CCO is considered to be "senior officer" eligible to approve the AML/CFT policies and procedures. While assigning this role to the CCO can help ensure proper integration of AML/CFT procedures into the firm's overall compliance procedures, Dealer Members should first assess the extent of the CCO's other duties. It is important for Dealer Members to keep up-to-date with AML/CFT rules and risks; a CCO having to deal with both day-to-day problems , changes to securities regulations and change to the PCMLTF requirements, among other requirements, may not have sufficient time to acquire and maintain the specialized knowledge that an effective AML/CFT regime needs.

5.5 Customer Due Diligence

The PCMLTF Regulations establish specific requirements for information gathering, customer identity verification and record keeping, generally grouped under the term "customer due diligence" (CDD). These are summarized in Appendix A.

The establishment of the customer-firm relationship often presents the best opportunity to begin to develop the firm's knowledge about the customer and the types of transactions in which the customer is likely to engage.

Dealer Members are accustomed to the basic KYC requirements mandated by IIROC Rules 1300, 2500 and 2700. In many instances the customer due diligence requirements for AML/CFT add little in the way of information to be gathered, but they require that it be looked at from a different angle: that of protecting the markets and the financial system rather than the customer. In this they are a form of gatekeeper, like the gatekeeper requirements in the Universal Market Integrity Rules (UMIR). This is not to suggest that Dealer Members should act as if all new customers should be treated with suspicion, merely that the process requires sensitivity to different issues and goals.

It is frequently at the account opening stage that Dealer Members identify suspicious activity or attempts to arrange suspicious transactions. Following are several indicators:

- A customer exhibits an unusual concern regarding the firm's compliance with government reporting requirements, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents;

- A customer wishes to engage in transactions that lack business sense, apparent investment strategy, or are inconsistent with the customer's stated business/strategy;

- A customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations;

- A customer appears to be acting as the agent for another entity but declines, evades or is reluctant, without legitimate commercial reasons, to provide any information in response to questions about that entity;

- A customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry; and

- A customer attempts to dissuade the firm from following its normal account opening procedures or attempts to have transactions executed immediately, before all the firm's normal checking and verification procedures can be completed.

Even if the firm decides not to open an account or conduct a transaction, it should consider whether it has reasonable grounds for filing an attempted suspicious transaction report. Further recommendations regarding the reporting of suspicious and attempted suspicious transactions are included in a separate section below.

5.6 Relationship Between Introducing and Carrying Brokers

Section 62(2)(o) of the PCMLTF Regulations was added in 2008 to cover introducing/carrying arrangements between dealers. It exempts from the CDD requirements "the opening of an account that is opened solely in the course of providing customer accounting services to a securities dealer." This places the CDD requirements solely on the introducing broker.

However, it is important to note that the exemption covers only the CDD provisions of the PCMLTF Regulations; it does not cover large cash transaction and suspicious transaction reporting.

However, because of a carrying broker's involvement in an introducer's account opening, transaction and record keeping processes, it is a good practice for the introducing/carrying agreement to specifically set forth the respective obligations relating to compliance with applicable AML/CFT laws and other applicable rules and regulations. The introducing broker needs to ensure it has all the tools necessary to fulfill the CDD requirements. The following should be considered:

- The must be a clear understanding between the introducing and carrying broker as to where the operational responsibility for all anti-money laundering procedures lies. Sufficient information must be available to those responsible for carrying out each procedure;
- If the carrying broker designs and provides the new account forms and other standard account documentation, it must ensure that it requests all the information and support all the processes necessary for the introducing firm to conduct full CDD;
- The carrying broker must provide reports necessary for introducing brokers to properly fulfill their transaction monitoring responsibilities;
- It should be clear what back-up support the carrying broker will provide, such as the checking of client names against terrorist lists;
- Electronic records maintained by the carrying broker must meet the record keeping and access requirements; and
- If customers can deal directly with the carrying firm to conduct transactions such as deposits, withdrawals and wire transfers, then there must be effective

communication between the firms to enable proper monitoring for suspicious activity.

Based upon the allocation of responsibilities and subject to a reasonable request by the introducing broker, carrying brokers may need to develop certain tools, or enhance existing tools, to assist the introducing broker in analyzing the transactional activity of its customers. These tools could include reports intended to assist the introducing firm in supervising and monitoring customer accounts, such as exception reports reflecting deposit and trading activity that might detect possible money laundering activity, including the structuring of deposits. Carrying brokers should include these reports on the list of reports required to be provided to introducing brokers at the inception of the introducing/carrying relationship.

Introducing and carrying brokers must also develop effective communications to deal with questionable activity or potential indications of suspicious activity. A carrying broker cannot, for example, consider its responsibilities fulfilled if it simply reports what it considers potentially suspicious activity to the introducing firm. The introducing broker should provide the carrier with sufficient information to satisfy itself that the activity has been appropriately dealt with, either through the filing of a suspicious transaction report or the receipt of an explanation sufficient to conclude that the activity gives no reason for suspicion. Feedback from the introducing broker can have the added benefit of either pointing at other activity that should be reviewed or preventing the recurrence of similar false positives.

The allocation of responsibilities should be made known to those conducting the annual audits of anti-money laundering procedures at both the introducing and the carrying firm. Those conducting the audits should be encouraged to work together and share information to ensure that there are no gaps and that both parties are properly executing their responsibilities as defined in the legislation, regulations and the introducing/carrying agreement.

5.7 Training

Section 71(1)(d) of the PCMLTF Regulations requires "a written ongoing compliance training program" for "employees, agents or other persons authorized to act on [a Dealer Member's] behalf."

A Dealer Member must train all new employees with respect to its anti-money laundering procedures, including the detection of unusual or suspicious transactions or attempted suspicious transactions and compliance with both federal and IIROC rules, regulations and reporting requirements. The firm's anti-money laundering policy should be made available to all new employees. In addition it is a good practice to incorporate it or references to it in other relevant firm materials, such as the firm's code of ethics or conduct.

Each Dealer Member should endeavour to tailor the contents of its anti-money laundering training to the specific needs and business of the organization. In so doing, the following themes should be addressed:

- The firm's KYC policy and procedures;
- The roles of salespeople, operations, supervisors, management and others,
- Potential indicators of suspicious activity;
- The rules and regulations for reporting currency transactions, transportation of monetary instruments and suspicious activity;
- The firm's procedures for reviewing unusual transactions and reporting suspicious transactions or activity; and
- The civil and criminal penalties associated with money laundering.

Firms should also periodically update their training materials to reflect recent developments, techniques or money laundering trends identified by various government agencies such as FINTRAC and FATF.

While general information about money laundering is useful, employees and agents should receive specific training about their role in the firm's anti-money laundering efforts. While salespeople having direct contact with clients may be in the best position to identify some forms of suspicious activity, other departments such as treasury, operations, margin, credit, corporate security, audit and legal and compliance need to understand what red flags might appear in the course of their daily activity.

The training program should take into account Dealer Member's money laundering risk assessment. The training program can also make use, with appropriate modifications or additions, of material developed for related purposes such as fraud prevention or the detection of market abuse. The training should cover the factors the types of clients, products or services the firm has assessed as being high risk, why they are high risk, the special controls implemented and relevant red flags. The results of a firm's AML audits may also identify areas of focus for the training program.

Employee training can take many forms, including live presentations, educational videos, on-line training programs or the use of other media. In addition, bulletins or other guidance documents can be distributed or circulated to employees firm-wide, or to select groups of employees as appropriate (i.e., registered representatives in particular business locations, cashier, margin, or operations personnel). Departments within the firm such as compliance, legal, internal audit, and human resources can all assist in developing the firm's training programs and in training firm personnel. There are outside course providers, but unless they tailor a course specifically for the Dealer Member, their offerings should be supplemented by training geared to the Dealer Member's business and the various roles assigned in its policies and procedures.

It is useful to use case examples in the course of training, focusing on what an employee or agent might see in a similar situation that should arouse their interest. These can be taken from past cases of suspicious or attempted suspicious transactions that occurred at the Dealer Member, suitably disguised, or from cases dealt with in typology studies such as those listed in the further reading section of this guidance.

Dealer Members should maintain evidence of who took the training and when to ensure that all employees have received the right training and as a basis for determining what their ongoing training should be.

Ongoing training can also be tailored to types of roles within the firm. Some employees may only need a refresher. Others may need training on new rules, programs, risks or changes in money laundering typologies and new red flags.

5.8 Review Program

The 2008 amendments to the PCMLTF Regulations changed the review requirement from "as often as necessary" to every two years. The review must cover the firm's:

- Policies and procedures;
- Risk assessment program; and
- Training program.

The review can be conducted by either internal personnel or an external party. As with all audits, it is important that the reviewers be independent of those principally responsible for the program, and have a thorough understanding of the AML/CFT requirements.

A report of the results has to be submitted to a senior officer[3] within 30 days of the review, and must include:

- Findings of the review;
- Any changes to AML/CFT policies and procedures made during the period of the review (i.e. since the last review); and
- The status of implementation of the changes.

The report should also outline measures undertaken to correct any weaknesses identified in the audit.

The report or a summary thereof should be included in the CCO's annual report to the Board on compliance matters required under IIROC Rule 38(h)(iv).

6. Suspicious Transactions Reports

6.1 Attempted Transactions

The 2008 amendments to PCMLTFA and related Regulations enhanced the suspicious transaction reporting requirements by including the reporting of attempted suspicious transactions, those in which a transaction proposed by a client was rejected by the firm.

Dealers Members' policies and procedures should provide guidance on how to deal with account applicants who raise suspicions. The guidance should address the following:

- Obtaining as much information from the applicant as possible;
- Methods for avoiding letting the applicant know that an employee is suspicious; and

[3] See definition above under "Written Anti-Money Laundering Procedures"

- Escalation procedures.

6.2 Completed Transactions

Each Dealer Member should have in place a monitoring program to review for unusual or potentially suspicious account activity. Depending upon the size and the nature of the firm's business, a monitoring program could take various forms, ranging from the manual monitoring of significant transactions or activity to the use of automated monitoring systems. Once the firm has determined the appropriate method to effectively monitor account activity, it should adopt appropriate related procedures.

As with other kinds of account supervision, exception reporting may be based on different factors such as the size of transactions and volume of activity.

Monitoring procedures should also be risk-based, focusing more attention on higher risk products, services and customers. However, low risk is not no risk and Dealer Members need to ensure that at least some attention is paid to all types of activity that could be related to money laundering or terrorist financing.

Suspicious activity can occur either at the outset of the client relationship or long after the relationship has been initiated. For longer-term clients, transactions should be viewed in the context of other account activity. A determination of whether the transaction is actually suspicious will depend on the customer and the particular transaction, compared with the customer's normal business activity. Unusual or questionable transactions may include transactions that appear to lack a reasonable economic basis or recognizable strategy based upon what the firm knows about the particular customer.

Examples of activity that may be indicative of unusual or potentially suspicious activity should be provided to all appropriate firm personnel and should be incorporated into the firm's anti-money laundering policies and procedures, as well as its anti-money laundering training materials.

Dealer Members should also make it clear to all employees that any suspicion that activities are related to crimes such as fraud and market manipulation is equivalent to a suspicion that they are related to money laundering and must be reported.

6.3 Other Monitoring Systems and Procedures

Dealers should recognize that there may be an AML/CFT aspect to issues raised by monitoring systems devoted primarily to compliance with other rules. It is also useful to note that it is nearly impossible to separate a transaction that is part of a market-based criminal offense from a transaction designed to launder the proceeds of the crime.

Gatekeeper reports filed with IIROC under UMIR Rule 10.16 on matters such as market manipulation or insider trading should be reviewed further to determine whether the transaction should also be reported to FINTRAC as suspicious of money laundering.

Improper activity by employees or agents such as internal theft or fraud or conspiracy with outside parties to manipulate a market should also be reviewed to determine whether it should result in suspicious transaction reports.

6.4 Examples of Indicators of Suspicious or Attempted Suspicious Activity

Although by no means exhaustive, the following is a list of potential indicators of suspicious activity which, if unexplained, may be linked to money laundering activity:

- A customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents or asks for exemptions to the firm's policies relating to the deposit of cash and cash equivalents;
- A customer engages in multiple transfers of funds or wire transfers to and from countries that are considered bank secrecy or "tax havens" that have no apparent business purpose or are to or from countries otherwise considered by the firm to be high-risk;

- A customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose;
- A customer deposits multiple third party cheques or securities registered to third parties;
- For no apparent reason, a customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers;
- An inactive account suddenly makes large investments or receives large amounts of funds inconsistent with the client's known financial position or normal investment practice;
- A customer uses an account to hold funds not used for investments for an extended period of time;
- A customer makes a funds deposit, for the purpose of purchasing a long-term investment, followed shortly thereafter by a request to liquidate the position and a transfer of the proceeds out of the account;
- Apparently unrelated customers direct funds to the same account or open unsolicited accounts to trade in the same security;
- An institutional account trades large volumes of a penny stock;
- A customer directs journal entry or other transfers of funds or securities between unrelated accounts without any apparent business purpose, including transfers to other dealers;
- A customer requests that a transaction be processed in such a manner so as to avoid the firm's normal documentation requirements;

- A customer engages in transactions involving certain types of securities, such as penny stocks, which, although apparently legitimate, have been utilized in connection with fraudulent schemes;

- A customer deposits bearer bonds followed by an immediate request for the disbursement of funds;

- A customer exhibits a total lack of concern regarding risks, commissions, or other transaction costs; and

- A customer engages in trading activity that appears to be manipulative, such as wash trading or directing the dealer to another dealer for an over-the-counter trade.

6.5 Suspicious Transaction Reporting

Dealer Members are required to file the following reports:

- Reports to FINTRAC on transactions or attempted transactions that give reasonable grounds to suspect money laundering or terrorist financing;

- Reports to FINTRAC, the Royal Canadian Mounted Policy and the Canadian Security Intelligence Service on property or transactions related to property of listed terrorists and terrorist groups; and

- Reports filed under the UN Suppression of Terrorism Regulations and other UN regulations.

Monitoring systems and procedures are designed to identify unusual activity, but firms must determine whether the activity gives reasonable grounds for suspicion. That judgment is best exercised by experienced personnel. Firm procedures should make clear that employees should report unusual activity, once detected, to managers or other supervisory personnel. Specific internal channels for reporting unusual or

suspicious activity should be established in the firm's policies and procedures. It is a good practice for the AML Officer to be at least aware of all suspicious transaction reports, and in many cases for the AML Officer to give approval to the filing of a report.

Those responsible for reviewing unusual transactions should conduct such additional enquiries as necessary to determine whether it is suspicious. For example, where the transactions are identified by automated monitoring, information may be available from the registered representative that explains the activity. However, when making enquiries those responsible should ensure that others do not warn the customer that his or her transactions are under scrutiny.

6.6 Dealing With Clients Who Have Conducted Suspicious Transactions

It is an offence to deliberately tell a client that the firm has filed a suspicious transaction report about his, her or its transactions. While the specific section of PCMLTFA, Section 8, requires that the disclosure be made "with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun," in practice it will be difficult to convince anyone that a client was told about a suspicious transaction report without such an intent.

Dealer Members should therefore have a procedure for dealing with clients whose activity have resulted in a suspicious transaction report. The following issues should be considered:

- What criteria may be used to determine whether the firm wishes to continue to deal with the client?
- Who will make the determination as to whether to continue dealing with the client?
- How will the client be told if the dealer decides not to continue dealing with him, her or it?

- What extra monitoring will be put in place if the dealer decides to continue dealing with the client?

- Is the suspicion sufficiently high to warrant a voluntary report to a criminal enforcement authority?

A report to a criminal enforcement authority could result in the dealer being asked to continue dealing with the client to assist in an investigation. Any such request should be made in writing. The dealer should also determine whether it will be obligated to continue making suspicious transaction reports regarding all of the client's future activity that might be connected to the investigation.

6.7 U.N. Suppression of Terrorism Reports and Similar Requirements

Dealer Members are required under the United Nations Suppression of Terrorist Regulations and United Nations Al-Qaida and Taliban Regulations to check client names against the lists of know terrorists and terrorist organizations. The lists and updates to them are available from the web site of the Office of the Superintendent of Financial Institutions at http://www.osfi-bsif.gc.ca/osfi/index_e.aspx?ArticleID=2523.

Reporting is to be conducted monthly through an automated system available through the IIROC Website:

http://ce.iiroc.ca/eis/General/WebForms/Login.aspx?ReturnURL=http%3a%2f%2funreport.iiroc.ca%2fdefault.aspx

From time to time other regulations are passed by the Federal Government adding to the basis for reporting. For example, special sanctions measures have been enacted to require checking of listed persons under regulations concerning Iran, North Korea, Burma and Zimbabwe.

Dealer Members should determine whether to periodically check all of the names on the lists or whether to supplement an initial check with a screening process for new

accounts and checks against the full account list of newly added persons and entities. A full check might be appropriate, for example, for a large dealer that opens many accounts and does periodic checks of all client names against lists of foreign politically exposed persons.

A Dealer Member doing periodic checks of all clients should implement a system for identifying false positives in order to avoid duplication of effort when the same clients come up again and again.

The regulations require that when an account is identified as that of a listed person, it be frozen and reported to the Royal Canadian Mounted Police, the Canadian Securities and Intelligence Service and FINTRAC.

Reporting is monthly through an automated system available through the IIROC Web site at http://ce.iiroc.ca/eis/General/WebForms/Login.aspx?ReturnURL=http%3a%2f%2funreport.iiroc.ca%2fdefault.aspx. Each Dealer Member must make a monthly "Nil" report if it has no accounts for listed persons or entities.

Access to the reporting system is password protected and limited to authorized persons at each firm. Dealer Members should have policies and procedures to ensure that the checks are done and reports filed on time, that there is a back-up for the person responsible for the reporting and that there is a succession plan and training in case that person leaves the firm.

7. Specific Issues

7.1 Third Party Transactions

Section 9(1) requires a Dealer Member opening an account to "take reasonable measures to determine whether the account is to be used by or on behalf of a third party.[4]" If there is a third-party involvement, the Dealer Member must record:

- The nature of the relationship between the third party and the accountholder; and
- An individual third party's name, address, date of birth and principal occupation or business; or
- An entity third party's name, address and principal business and, if the entity is a corporation, its incorporation number and place of issue.

If the Dealer Member is unable to determine that the account will be used by or on behalf of a third party but has reasonable grounds to suspect that it will, the Dealer Member is required to keep a record of what the person who has authority over the account has disclosed about whether it will be used by or on behalf of a third party and describes the reasonable grounds to suspect that it will be.

Third party transactions should be distinguished from beneficial ownership, described below. The named client is the owner of the account and all transactions conducted through the account are presumed to belong to and be for the owner. Where the client is an entity such as a corporation or trust, the transactions are presumed to belong to and be for the benefit of the entity. While there may be beneficial owners or beneficiaries of the entity, the entity is the direct client and owner of the account.

A third party transaction is one for the benefit of someone other than the named client. It may be one transaction out of many done in the account; or different transactions

[4] Section 8(1) contains a similar provision regarding large cash transactions. This guidance will not deal with that requirement as most Dealer Members do not accept large cash transactions.

could be done for different third parties. However, this does not make the third parties owners or part owners of the account. It is possible, for example, for a corporate account to do a transaction on behalf of a part owner of the corporation. If the transaction is solely for the benefit of that part owner, not the corporation, it is a third party transaction.

There are obvious cases in which some or all of the transactions for an account will be for third parties, the most obvious being transactions done by other dealers that act as agents for clients. For each trade there is a third party: the client of the other dealer.

The regulations provide exceptions from the section 9(1) requirements for accounts of the following:

- Financial entities as defined in PCMLTFA, i.e. banks (including the Canadian operations of foreign banks authorized under section 2 of the *Bank Act*), trust companies, credit unions, and caisses populaires;
- A securities dealer engaged in the business of securities dealing in Canada. For this purpose, registered Portfolio Managers are considered securities dealers;
- A lawyer, accountant or real estate broker or sales representative using the account only for his, her or its clients; and
- Entities engaged in the business of dealing in securities solely outside of Canada, subject to conditions set out below under "Accounts of Financial Institutions."

Most retail new client application forms contain questions similar to the IIROC Form 2 questions asking whether others have trading authority over or a financial interest in the account. Absent any indicators to the contrary, asking the question and getting a "no" answer will generally be considered to be a reasonable measure. Indicators to the contrary may include:

- Deposits of cheques or securities from third parties;

- Issuance of cheques to third parties;
- Transfers of funds or securities from or to the accounts of third parties;
- Instructions being given by third parties, particularly where the third party is given full power of attorney to order movements of funds and securities to and from the account; and
- Registration of securities in the names of third parties.

Although, there can be many reasons for such transactions where there is a known relationship between the named client and the third party, enquiries should be made if the circumstances suggest that the original transaction was done on behalf of the third party. Where there is no known relationship between the parties, extra due diligence should be undertaken to determine the reasons for the transaction and whether the account is being used for third-party transactions.

In some cases, sales assistants or operations staff may notice transactions with indications that an undisclosed third party may be involved with the account or transaction. These kinds of transactions will often occur after an account has been in operation for a specific period. These personnel should refer the issue to the Registered Representative, Compliance Department or designated AML Officer.

If the client does disclose a third-party involvement, the representative should make follow-up enquiries to obtain the required information, with particular stress on the nature of the relationship between the parties. There are legitimate reasons that a third party might have an interest in a trade in another person's or entity's account. Such transactions may be problematic for reasons other than AML/CFT, such as the third party's residence in a jurisdiction in which the representative or firm is not permitted to trade.

7.2 Beneficial Ownership

Money launderers and market abusers have often used corporations and other non-person accounts to shield their identity and make it more difficult to identify and investigate their improper or illegal conduct.

The IIROC Dealer Member Rules regarding the identification of beneficial owners of corporations and other entities were implemented to both deter money laundering through such entities and to assist in investigations of market conduct. The IIROC Rules were implemented first and in some ways are more stringent than the PCMLTFA Regulations. As with any other overlapping rules, compliance with the strictest rules is required.

IIROC Rule 1300.1(b) (1) requires a Dealer Member to:

> ascertain the identity of any individual who is the beneficial owner of, or exercises direct or indirect control or direction over, more than 10% of the corporation or similar entity, including the name, address, citizenship, occupation and employer of each such beneficial owner, and whether any such beneficial owner is an insider or controlling shareholder of a publicly traded corporation or similar entity

It is important to note that the IIROC Rule refers to direction or control as well as beneficial ownership. As part of its due diligence, a Dealer Member should understand the ownership and control structure of any corporation or other entity that opens an account. In some corporations ownership may be split from control, for example where a corporation has both voting and non-voting shares. In the case of trusts, the trustees have direction or control without being the beneficiaries.

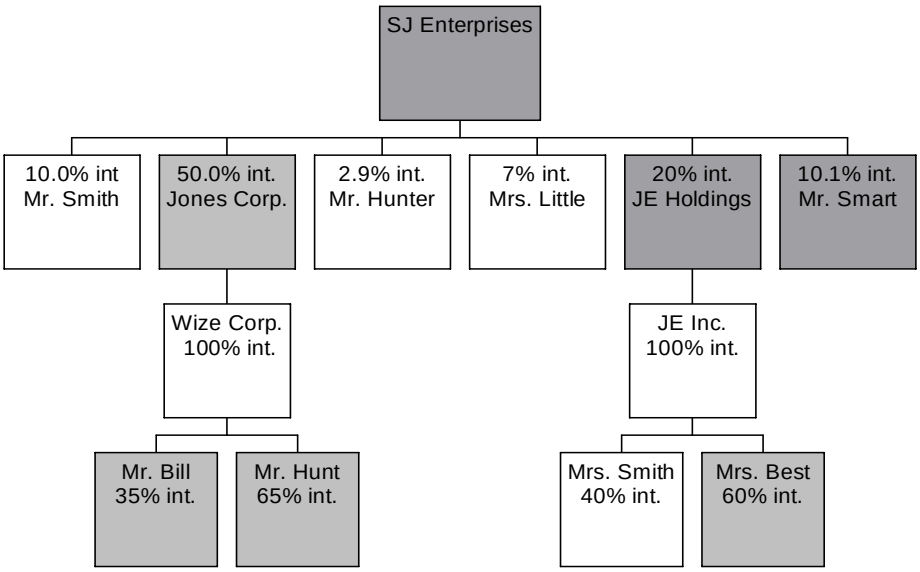
The rule refers to "direct or indirect" ownership, direction or control by individuals. Where a corporate client is owned or controlled by other corporations or other entities, the Dealer Member is required to go behind those other entities to identify the

individuals who ultimately have the beneficial ownership or control. Where a corporate client has more than one owner, the Dealer Member should identify the extent of the ownership or control of each individual involved.

In some cases the determination of an individual's ownership interest will be straightforward. For example, if an individual owns 40% of a corporation that owns 10% of the accountholder corporation, the individuals ownership interest in the accountholder is 4% so the individual falls below the threshold in the rule.

However, the issue of direction or control may not be so straightforward.

The following example shows the calculation of percentage indirect ownership in a multi-level ownership structure:



Natural Person	Ownership Calculation (of SJ Enterprises)	Is Beneficial Ownership Information Required?
Mr. Bill	0.35 X 1.00 X 0.50 = 0.175 = 17.5%	Yes
Mr. Hunt	0.65 X 1.00 X 0.50 = 0.325 = 32.5%	Yes
Mrs. Smith	0.40 X 1.00 X 0.20 = 0.080 = 8.00%	No
Mrs. Best	0.60 X 1.00 X 0.20 = 0.120 = 12.0%	Yes
Mr. Smith	10.0%	No
Mr. Hunter	2.9%	No
Mrs. Little	7.0%	No
Mr. Smart	10.1%	Yes

Section 11.1 of the PCMLTF Regulations requires that dealers obtain the name, address and occupation of anyone owning, directly or indirectly, more than 25% of a corporation or other entity. Therefore by complying with the IIROC Rule a Dealer Member will comply with the PCMLTF Regulations.

However, the IIROC Rule requires that Dealer Members verify the identity of beneficial owners where the PCMLTF Regulations do not. The IIROC Rule is principles based. It does not dictate any specific method of verifying the identity of beneficial owners; instead, it requires that the Dealer Member use "such methods as enable the Dealer Member to form a reasonable belief that it knows the true identity of each individual and that are in compliance with any applicable legislation and regulations of the Government of Canada or any province." Because the PCMLTF Regulations do not require verification of the identity of beneficial owners, there are no applicable regulations of the Government of Canada.

Dealer Members are therefore free to use any methods of identity verification that will enable them to form a reasonable belief that they know the beneficial owner's true identity. There are two aspects to verification:

- Who actually owns the corporation or other entity? The Dealer Member must make the necessary enquiries of the corporation, but is entitled to take the corporations word on who the beneficial owners are unless there is any reason to be suspicious that the information is not accurate; and

- Are they who they say they are? The member needs to take reasonable steps to verify the identity of each beneficial owner or person controlling the account. In many cases the Dealer Member may already have verified the identity of the owner if the owner has personal accounts at the firm. Any of the methods identified in the PCMLTF Regulations is acceptable for the purposes of identity verification under IIROC Rule 1300, including use of only one of the methods in Schedule 7 of the PCMLTFA Regulations for non-face-to-face verification.

Members can also consult other sources of information or accept less formal means of identification such as copies including faxed copies of identity documents. However, care should be used with the latter, particularly where a corporate account is high risk. To reiterate, the means has to enable the Dealer Member to form a "reasonable belief" that it knows the identity of the beneficial owner; whether such a belief is reasonable will be dictated by circumstances. It may not be reasonable where there are numerous red flags about the corporation or the type of activity in which it wishes to engage.

The IIROC Rule requires that the verification of beneficial owners be done "as soon as is practicable after opening the account, and in any case no later than six months after the opening of the account." The PCMLTF Regulations require that the existence of the corporation or other entity be verified with 30 days of account opening. Therefore, the only part of the verification process that can go beyond the 30 days is the verification of the identity of beneficial owners under the IIROC Rule. However, it is important to note that the IIROC rule requires that verification to be done "as soon as practicable." The six months is the maximum permitted timeframe, but Dealer Members are expected to begin efforts to verify the identity of beneficial owners at the time of account opening, not wait for six months.

The PCMLTF Regulations permit a Dealer Member to open an account for a corporation or other entity even if it can't ascertain the beneficial owners provided that it maintains a record of the reason it could not do so. However, IIROC Rule 1300.1(g) prohibits a Dealer Member from opening an account for a corporation or other entity when it

cannot obtain the beneficial ownership information. Because the IIROC Rule is more stringent, Dealer Members are not permitted to open an entity account without ascertaining the beneficial owners.

If it does get the beneficial ownership information but is unable to verify the identity of the beneficial owners within six months, the Dealer Member must limit the account to liquidating trades, transfers out and payments out until it completes the verification.

Any case in which the Dealer Member cannot obtain the necessary information about the customer and complete the necessary verification should be viewed as unusual and scrutinized for possible reporting of suspicious transactions or attempted suspicious transactions.

IIROC Rule 1300.1 contains the same provisions for identification and verification of identity of settlors of trusts and known beneficiaries of more than 10% of trusts. Testamentary and publicly traded trusts are exempted. Trusts are not singled out in the PCMLTF Regulations, but come under the general term "entities." The threshold for beneficiaries under the PCMLTF Regulations is 25%.

Dealer Members should document the nature of the trust relationships, but are entitled, in the absence of any circumstances raising suspicion, to accept information from trustees or settlors without obtaining the documents establishing the trust.

7.3 Accounts of Financial Institutions

The identification and verification requirements for financial institutions are complex, particularly regarding off-shore institutions. There are again differences between the exemptions for financial institutions in the PCMLTF Regulations and those in the IIROC rules. The PCMLTF Regulations contain blanket exemptions from CDD requirements only for Canadian financial institutions; the exemptions in the IIROC rules are broader.

Full details of how the regulations apply to different types of clients are included in Appendix A. This discussion is meant to highlight some of the distinctions that Dealer Members should be aware of.

The three critical features to be determined in relation to any financial institution exemption are:

- Is the particular institution exempt at all?

  The PCMLTF Regulation exemptions are generally available only for Canadian financial institutions. However, even that general statement needs to be handled carefully, since the Canadian operations of "authorized foreign banks within the meaning of Section 2 of the *Bank Act*" are included under the exemptions.

- What provisions it is exempt from?

  There are exemptions from customer due diligence requirements in general and narrower exemptions. Where a financial institution is exempt from information gathering requirements under the PCMLTF Regulations, it is also exempt from identity verification requirements. On the other hand, as described below, foreign dealers that are exempt from identifying the clients for whom they are acting are not exempt from the customer due diligence requirements with regard to the dealer itself.

- What are the conditions, if any, under which the exemption is available?

  For example, several exemptions are conditional on the financial institution being located in a FATF member country or a non-FATF country that is in compliance with the FATF recommendations.

One important exemption for Dealer Members is limited in scope: the exemption from third-party identification for foreign securities dealers. The exemption covers only the need to identify the third parties, (i.e. clients for whom foreign securities dealers enter

orders. It does not cover the need to gather the required information about the entity including beneficial ownership, verify its existence and verify the identity of those authorized to give instructions for it.

It is also important to note that the exemption covers a person or entity "engaged in the business of dealing in securities only outside of Canada." It is phrased in terms of being in the business of dealing in securities, so that it covers other types of institutions that deal in securities in other countries, such as banks.

The exemption for foreign securities dealers also illustrates the conditional nature of some exemptions. It is available for those dealing in securities:

- In FATF member countries (see Appendix E), or
- In non-FATF member countries that have implemented the FATF customer due diligence recommendations, provided that the foreign dealer certifies in writing that it has implemented the recommendations.

If neither of these conditions applies to the country, the Dealer Member does not need to identify the third party for a specific transaction if it has verified the identity all the third parties the dealer acts for, i.e. the foreign dealers full client list. Since the latter is impractical the Dealer Member will generally have to identify the underlying client in any transactions for dealers in such countries.

For countries that are not FATF members, it is left to the dealer to determine the extent of the country's implementation of the FATF customer due diligence recommendations.

The FATF is no longer maintaining a list of non-compliant countries and territories; however, the country evaluations by FATF, FATF-style regional bodies and the International Monetary Fund all comment on the evaluated country's compliance with the 40 recommendations. The FATF evaluations show whether a country is compliant, non-compliant or partially compliant with each recommendation. These evaluations

can be found on the FATF Web site (http://www.fatf-gafi.org), or on the web sites of the FATF-style regional bodies, which can be found through links on the FATF Web site.

In making a determination, a Dealer Member should place particular emphasis on the country's compliance with Recommendation 5 on Customer Due Diligence. If the country is partially compliant with the recommendation, the Dealer Member should review the details of the evaluation to ascertain the extent of the non-compliance to determine whether it is minor and technical or results of significant deficiencies in the regime.

The IIROC rules exempt financial institutions subject to a satisfactory AML regime from the beneficial ownership requirements. For this purpose, a Dealer Member is permitted to use the criteria for determining that a country has a satisfactory regulatory regime used in the PCLMTF Regulations as described above.

Another exemption under the PCMLTF Regulations that may be available for a foreign financial institution is the public company exemption in section 62(2)(m) of the PCMLTF Regulations for "a corporation that has minimum net assets of $75 million on its last audited balance sheet and whose shares are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the *Income Tax Act*, and operates in a country that is a member of the Financial Action Task Force." This exemption is from all CDD and also applies, under subsection 62(2)(n) to subsidiaries of such public companies whose financial statements are consolidated with those of the listed entity.

The stock exchanges listed under subsection 262(1) that operate in FATF member countries are listed in Appendix G.

7.4 Politically Exposed Foreign Persons

Sections 9.3(1) of PCMLTFA and section 57.1(1) of the PCMLTF Regulations require Dealer Members to take reasonable measures to ascertain whether a new client is a

"politically exposed foreign person" (PEFP). These measures must be taken within 14 days of opening an account. The definition of a PEFP is found in section 9.3(3) of PCMLTFA as follows:

- A person who holds or has held one of the following offices or positions in or on behalf of a foreign state:
    - head of state or head of government;
    - member of the executive council of government or member of a legislature;
    - deputy minister or equivalent rank;
    - ambassador or attaché or counsellor of an ambassador;
    - military officer with a rank of general or above;
    - president of a state-owned company or a state-owned bank;
    - head of a government agency;
    - judge;
    - leader or president of a political party represented in a legislature; or
    - holder of any prescribed office or position. At present there are no such prescribed officers or positions.
- Any prescribed family member of such a person. The prescribed family members under section 1.1 of the PCMLTF Regulations are:
    - the person's spouse or common-law partner;
    - a child of the person;
    - the person's mother or father;

- the mother or father of the person's spouse or common-law partner; and
- a child of the person's mother or father.

There is at present little guidance regarding what is considered to be a reasonable measure to determine whether a client is a PEFP (FINTRAC Guideline 6E(7.1)). In most cases where it is highly unlikely that the client is a PEFP it will be enough to ask the question. However, the question – whether asked verbally or put on a new account form to be completed by the client – should include a description of what a PEFP is. It need not be as detailed as the above but should be detailed enough to enable the Dealer Member to identify situations warranting further enquiry.

Firms with large numbers of customers that do international business should consider making use of one of the services that checks customers against lists of known politically exposed persons, not only when an account is open but on an ongoing basis to ensure that none of their existing clients have become or been newly identified as PEFPs.

Ongoing checking or "scrubbing" of client names is likely to yield repeated false positives, so dealers who do periodic checks are well advised to have a process to ensure that they don't duplicate checks on those false positives.

Firms that do not use such services to check all accounts can use some of them on a single enquiry basis when the firm has a concern about a particular client.

When a customer is identified as a PEFP, the Dealer Member must:

- Take reasonable measures to establish the source of the funds that have been, will be or are expected to be deposited in the account.
- Obtain the approval of senior management to open or continue to operate the account. The member or members of senior management who are permitted to authorize the opening of a PEFP account should be designated in the firm's

policies and procedures. If it is not the designated AML Compliance Officer he/she should nonetheless be informed of the opening of a PEFP account.

- Conduct enhanced ongoing monitoring of the account to detect suspicious transactions.

The PEFP requirements are directed at preventing laundering of the proceeds of corruption. In opening an account for a PEFP a firm should examine carefully the purpose of the account and how it came to be opened. The firm should determine what additional due diligence or monitoring are necessary.

Additional due diligence may include direct enquiries of the customer regarding source of funds, verification of details given by the client though outside sources and other checks to determine whether there is a reasonable basis for believing that the client's assets were legitimately derived. Additional monitoring can include reviews of asset levels to ensure that they are and remain reasonable in light of what is known about the client's legitimately-derived financial means and regular reviews for transactions that are not in keeping with the stated purpose of the account or normal investment practice.

The FATF Interpretive Note to Recommendation 6 suggests that a country consider applying the same rules to domestic politically exposed persons (PEP) as to foreign ones. While Canada has chosen not to follow that suggestion, Dealer Members should consider political exposure in its risk assessments of particular clients, whether or not the person is a PEFP under the PCMLTFA definition. This includes not only domestic political exposure, but also those holding similar positions at lower levels of government such as state, provincial or municipal governments.

Similarly, there is no requirement to determine whether the directors or beneficial owners of corporation or other entity accounts are politically exposed persons. Nonetheless, it is good practice to ask the contact at the entity and, if the Dealer

Member uses an outside service to check for political exposure, run the names of senior officers, directors and beneficial owners.

A Dealer Member is not required to go through the same process of senior management approval when they identify a client as a domestic PEP, a PEP a lower than national level of government or a corporation or other entity associated with, or partly owned by, a PEP or PEFP. However, the Dealer Member should consider the extent to which additional approval, due diligence or monitoring is warranted in such cases to deal with the risks associated with such accounts.

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 1: ACCOUNTS OF INDIVIDUALS

Requirement and Reference	Details
Information to be obtained PCMLTF Reg. 23(1)	• Name • Address • Date of birth • Occupation • Intended use of the account • Whether the individual is a PEFP[5] and, if so: o The office or position in respect of which the person is a PEFP o The source of funds deposited or expected to be deposited in the account o Date of determination that the person was a PEFP o Name of the member of senior management that approved keeping the account o Date of above approval
Signature document PCMLTF Reg. 23(1)(a)	Signature card, account operating agreement or account application bearing the signature of the person authorized to give instructions for the account
Large cash transaction records PCMLTF Regs. 1, 3, 4, 5, 8, 21, 22	**Process:** Report to FINTRAC receipt from a client of $10,000 or more in cash the course of a single transaction (including two or more transactions in the course of a rolling 24 hour period) on Schedule 1 within 15 days of the transaction **Records required:** Large cash transaction record of above including: • Person from whom the cash is received, if the information is not readily available from other records • Name • Address • Date of birth • Nature of principal business or occupation • Date and of deposit • Account number, name, type and currency of any account affected by the transactions • Purpose and details of the transactions • Whether the cash is received by armoured car, in person, by mail or some other way • Amount and currency

[5] A person who holds or has held one of the following offices or positions in or on behalf of a foreign state:
(a) head of state or head of government; (b) member of the executive council of government or member of a legislature;
(c) deputy minister or equivalent rank; (d) ambassador or attaché or counsellor of an ambassador;
(e) military officer with a rank of general or above; (f) president of a state-owned company or a state-owned bank;
(g) head of a government agency; (h) judge; (i) leader or president of a political party represented in a legislature
And, in respect of any of the above:
(a) the person's spouse or common-law partner; (b) a child of the person; (c) the person's mother or father;
(d) the mother or father of the person's spouse or common-law partner; and (e) a child of the person's mother or father.

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 1: ACCOUNTS OF INDIVIDUALS

Requirement and Reference	Details
Third party information (disclosed by client) PCMLTFA Reg. 9(2)	**Records of individual third party required:** • Name • Address • Date of birth • Principal business or occupation • Relationship between the individual and the third party **Records of entity third party required:** • Name • Address • Nature of principal business • If a corporation, incorporation number and place of issue • Relationship between the individual and the entity
Third party information (reasonable grounds to suspect but not determined) PCMLTFA Reg. 9(3)	**Records required:** • What the individual says about third party use • Grounds for suspecting third party involvement
Exceptions to third party information PCMLTF Reg. 9(6)	Account opened by any of the following if the dealer has reasonable grounds to believe it will be used only the clients of the individual: • Legal counsel • Accountant • Real estate broker or sales representative

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 1: ACCOUNTS OF INDIVIDUALS

Requirement and Reference	Details
Exceptions to identity verification PCMLTF Reg 62.	• Existing clients whose identity has previously been verified • Individuals authorized to trade in corporate or other entity accounts if the identities of three authorized individuals have already been verified • New accounts, generally transfers, if the RR or assistant personally verified the client's identity at the previous firm. However, the RR must provide some record of when and how that was done. • An account opened solely to deposit and sell shares acquired from a corporate demutualization or privatization of a Crown corporation. If the proceeds are to be kept for further investment, the client's identity has to be verified. • Registered accounts such as RRSPs, RRIFs, LIRAs, etc. • Escrow accounts established under Canadian stock exchange or securities regulatory requirements • Accounts carried for another Canadian securities dealer, adviser or portfolio manager • An account opened solely for the sale of mutual funds (or a series of transactions including that sale) where there are reasonable grounds to believe that the client's identity has previously been verified by a securities dealer • An account opened solely for: o The purchase of an immediate or deferred annuity that is paid for entirely with funds that are directly transferred from a registered pension plan or from a pension plan that is required to be registered under the Pension Benefits Standards Act, 1985, or similar provincial legislation o The purchase of a registered annuity policy or a registered retirement income fund o The purchase of an immediate or deferred annuity that is paid for entirely with the proceeds of a group life insurance policy o A transaction that is part of a reverse mortgage or of a structured settlement • An account in respect of which instructions are authorized to be given by a Canadian: o Financial entity o Securities dealer o Life insurance company • Any individual member of a group RRSP plan in which the: o Member's contributions are made by the sponsor of the plan or by means of payroll deductions and o Existence of the plan sponsor has been verified
Exception to PEFP identification PCMLTF Reg.	Any individual member of the group plan in which the: • Member's contributions are made by the sponsor of the plan or by means of payroll deductions and • Existence of the plan sponsor has been verified

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 1: ACCOUNTS OF INDIVIDUALS

Requirement and Reference	Details
Identity verification: Timing PCMLTF Reg. 64(2)(a)	Before any transactions other than an initial deposit
Identity verification: Face-to-Face PCMLTF Reg. 64(1)(a) PCMLTFA Reg. 67(a)	**Process:** Review original and currently valid (i.e. unexpired) identification document. Any of the following is acceptable: • Passport • Driver's license • Provincial health card if provincial law permits it to be used as a means of identification (prohibited in Ontario, Manitoba and PEI, permitted in Quebec but you may not ask for it, only accept it if proffered by the individual) • Canadian record of landing or permanent resident card • Certificate of Indian status • A card with the individual's signature and photograph on it, issued by any of the following: o Insurance Corporation of British Columbia o Alberta Registries; o Saskatchewan Government Insurance; o Department of Service Nova Scotia and Municipal Relations o Department of Transportation and Public Works of the Province of Prince Edward Island o Service New Brunswick o Department of Government Services and Lands of the Province of Newfoundland and Labrador o Department of Transportation of the Northwest Territories o Department of Community Government and Transportation of the Territory of Nunavut • Government-issued age of majority cards **Records required:** • Type of document • Reference number • Place of issue **Note:** Credit cards and bank debit cards are not an acceptable means of identification
Identity verification: By agent or mandatary PCMLTF Reg. 64.1	**Process:** Face-to-face verification as above by the agent or mandatary **Records required:** • Written agreement or arrangement with agent or mandatary • Customer information obtained by the agent or mandatary

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 1: ACCOUNTS OF INDIVIDUALS

Requirement and Reference	Details
Identify verification: By affiliate PCMLTF Reg. 64(1)(b)(i) PCMLFT Reg. 64(1.2) PCMLTF Reg. 67(d)	**Process:** • Confirm that an affiliate has conducted a face-to-face verification as above • Verify that the name, address and date of birth in the record kept by the affiliate corresponds to the information obtained from the customer by the dealer **Eligible affiliates:** • An authorized foreign bank under section 2 of the Bank Act in respect of its business in Canada • A bank to which the Bank Act applies • Cooperative credit societies, savings and credit unions and caisses populaires regulated by provincial Act and associations regulated by the Cooperative Credit Associations Act • Life companies or foreign life companies to which the Insurance Companies Act applies or regulated by provincial Act • Companies to which the Trust and Loan Companies Act applies • Trust companies regulated by provincial Act • Loan companies regulated by provincial Act • Securities dealers • An entity carrying on activities outside Canada similar to any of the above where: o The dealer wholly owns the affiliate o The affiliate wholly owns the dealer, or o Both are wholly owned by the same entity. **Records required:** • Name of the affiliate • Type and reference number of the document the affiliate relied upon

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 1: ACCOUNTS OF INDIVIDUALS

Requirement and Reference	Details
Identity verification: Not face-to-face PCMLTF Reg. 64(1)(b)(ii), 67(b)(c)(e)(f) and (g) and Schedule 7	**Process:** Two of the following methods in any of the following combinations: • Identification product and attestation • Identification product and cleared cheque • Identification product and confirmation of deposit account • Credit file and attestation • Credit file and cleared cheque • Credit file and confirmation of deposit account • Attestation and cleared cheque • Attestation and confirmation of deposit account **1. Identification Product Method** **Process:** Refer to an independent and reliable identification product based on personal information in respect of the person and a Canadian credit history of the person of at least six month's duration. **Records required:** • Name of the identification product and provider • Search reference number • Date the product was used to ascertain the person's identity **Note:** Identification products are offered by commercial entities such as credit reporting agencies. **2. Credit File Method** **Process:** • Obtain the individual's permission to access their credit file • Confirm their name, address and date of birth from the credit file, which must be in Canada and must have been in existence for at least six months **Records required:** • Name of the credit reporting agency • Date the file was reviewed Continued...

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 1: ACCOUNTS OF INDIVIDUALS

Requirement and Reference	Details
	3. Attestation Method **Process:** Obtain from the client an attestation from a commissioner of oaths in Canada, or a guarantor in Canada, that they have seen one of the documents acceptable for face-to-face verification. **Acceptable guarantors:** Anyone engaged in any of the following professions in Canada: • Dentist • Medical doctor • Chiropractor • Judge • Magistrate • Lawyer • Notary (in Quebec) • Notary public • Optometrist • Pharmacist • Professional accountant (APA [Accredited Public Accountant], CA [Chartered Accountant], CGA [Certified General Accountant], CMA [Certified Management Accountant], PA [Public Accountant] or RPA [Registered Public Accountant]) • Professional engineer (P.Eng. [Professional Engineer, in a province other than Quebec] or Eng. [Engineer, in Quebec]) • Veterinarian **Records required:** A legible photocopy of the document including the: • Name, profession and address of the person providing the attestation • Signature of the person providing the attestation • Type and number of the identifying document provided by the person Continued...

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 1: ACCOUNTS OF INDIVIDUALS

Requirement and Reference	Details
	4. Cleared Cheque Method **Process:** Confirm that a cheque drawn by the person on a deposit account in the person's name at one of the following has cleared: • An authorized foreign bank within the meaning of section 2 of the Bank Act in respect of its business in Canada • A bank to which the Bank Act applies • A cooperative credit society, savings and credit union or caisse populaire that is regulated by a provincial Act • An association that is regulated by the Cooperative Credit Associations Act • A company to which the Trust and Loan Companies Act applies • A trust company or loan company regulated by a provincial act • A deposit-taking department or agency of the Government of Canada or of a province. **Records required:** Copy of the cleared cheque showing the name of the entity on which it was drawn and the account number **5. Confirmation of Deposit Account Method** **Process:** Confirm that the person has a deposit account with any of the financial entities for which the cleared cheque method is acceptable **Records required:** • Name of the financial entity where the account is held • Number of the account • Name and position of the person at the financial entity who gave the confirmation • Date of the confirmation

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 2: ACCOUNTS OF CANADIAN FINANCIAL INSTITUTIONS AND PUBLIC BODIES

Requirement and Reference	Details	Account Type
PCMLTF Reg. 62(2)(j)		**Exempted from large cash transaction report requirements** • Financial entity: o Bank under the Bank Act o Authorized foreign bank re its business in Canada o Provincially or federally regulated cooperative credit society, credit union, caisse populaire, trust company or loan company o Federal or provincial department or agency carrying out deposit-taking business with the public
PCMLTF Reg. (m)		• Public body: o Any department or agent of Her Majesty in right of Canada or of a province o An incorporated city, town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body or an agent of any of them o An organization that operates a public hospital and that is designated by the Minister of National Revenue as a hospital authority under the Excise Tax Act, or any agent of such an organization
PCMLTF Reg. 62(2)(h)	Same as requirements in Appendix A, Table 1	**Not exempted from large cash transaction report requirements** • Affiliate of a financial entity that is engaged in any of the activities of a financial entity or a securities dealer. (Note: "Affiliate" is not defined. Where it appears elsewhere, it is defined by full ownership of one entity by the other or of both by a common parent.)
PCMLTFA Reg. 62(2)(j)		• Securities dealers under provincial legislation, including advisers and portfolio managers
PCMLTF Reg. 62(2)(l)		• Life insurance company or foreign life insurance company to which the Insurance Companies Act applies or a life insurance company regulated by a provincial Act
PCMLTF Reg. 62(2)(m)		• Corporation with minimum net assets of $75 million on its last audited balance sheet whose shares are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the Income Tax Act in a country that is a member of the Financial Action Task Force (see Appendix E)
PCMLTF Reg. 62(2)(n)		• Subsidiary of a public body whose financial statements are consolidated with those of the public body
PCMLTF Reg. 62(2)(k)		• Pension fund regulated by or under an Act of Parliament or of the legislature of a province
PCMLTF Reg. 62(2)(l)		• Investment fund regulated under provincial securities legislation

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 3: FOREIGN SECURITIES DEALERS

Requirement and Reference	Details
Information to be obtained PCMLTF Regs. 23(1), 57(3)	• Name • Address • Nature of principal business • Intended use of the account
If a corporation, management information to be obtained PCMLTF Reg. 11.1 (1)(a)	All directors: • Name • Occupation
Beneficial ownership PCMLTF Reg. 11.1(1)(a) IIROC Rule 1300.1(b)(i) PCMLTF Reg. 11.1(1)(b) IIROC Rule 1300.1(c)(i)	If subject to a satisfactory regulatory regime in the country in which it is located • Corporation - individuals owning or controlling, directly or indirectly, more than 25% of the shares: o Name o Address o Occupation • Other entity - individuals owning or controlling, directly or indirectly, more than 25% of the entity: o Name o Address o Occupation **Timing:** At the time of verification of the existence of the entity (i.e. within 30 days of account opening) If not subject to a satisfactory regulatory regime in the country in which it is located • Individuals owning or controlling, directly or indirectly, more than 10% of the corporation or entity: o Name o Address o Citizenship o Occupation o Employer
Signature document PCMLTF Reg. 23(1)(a)(i)	Signature card, account operating agreement or account application bearing the signature of the person authorized to give instructions for the account
If a corporation, other documents PCMLTF Reg. 31(1)(b)	**Process:** Copy of the part of official corporate records that contains any provision relating to the power to bind the corporation in respect of the account. (i.e. Corporate Resolution)

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 3: FOREIGN SECURITIES DEALERS

Requirement and Reference	Details
Verification of the existence of the entity PCMLTF Regs. 57(3), 65(1) PCMLTF Regs. 57(4), 66(1) PCMLTF Regs. 65(2)(d), 66(2)(d) PCMLTF Regs. 65(3), 65(4), 66(3), 66(4)	**Process:** • Corporation o Certificate of corporate status o A record that it is required to file annually under the applicable provincial securities legislation; or o Any other record that ascertains its existence as a corporation • Other entity o Partnership agreement o Articles of association; or o Other similar record that ascertains its existence The record may be in paper form or in an electronic version that is obtained from a publicly accessible source. **Timing:** Within 30 days of account opening **Records required:** • Paper copy of record referred to, or • Electronic record o Registration number o Type of record referred to o Source of the electronic version of the record
Identity verification: Individuals authorized to give instructions PCMLTF Regs. 57(1), 62(a)	Verification of up to three individuals authorized to give instructions for the account **Process:** Methods described in Table 1 for individuals **Timing:** Before conducting any transactions other than an initial deposit **Records:** Records described in Table A for individuals
Exemptions from identity verification of individuals authorized to give instruction PCMLTF Reg. 62(2)(h)	Affiliate of a financial entity
Identity verification of beneficial owners IIROC Rule 1300.1(b)(ii)	If not subject to a satisfactory regulatory regime in the country in which it is located **Process:** Any method that enables the Dealer Member to form a reasonable belief that it knows the true identity of each individual **Timing:** As soon as practicable and in any event no later than 6 months after account opening

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 3: FOREIGN SECURITIES DEALERS

Requirement and Reference	Details
Third party information PCMLTF Regs. 9(1), 9(2), 9(5)	**1. FATF Member country** No requirement **2. FATF observer country** (Not a FATF Member country but has implemented the FATF Recommendations regarding customer identification) No requirement if the Canadian dealer obtains from the foreign dealer, at the time the account is opened, written assurance that the country where the foreign dealer is located has implemented the FATF customer identification recommendations. **3. FATF non-compliant country** (Not a FATF Member country and has not implemented the FATF Recommendations on customer due diligence) • Third party in each transaction • Records of individual third party required o Name o Address o Date of birth o Principal business or occupation o Relationship between the individual and the third party • Records of entity third party required o Name o Address o Nature of principal business o If a corporation, incorporation number and place of issue o Relationship between the individual and the entity
Large cash transaction records PCMLTF Reg. 21	Same requirements as in Table 1

Note: These requirements do not apply to a foreign securities dealer that is exempt from the CDD and verification requirements by virtue of being a corporation that has minimum net assets of $75 million on its last audited balance sheet and whose shares are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the *Income Tax Act (see Appendix F)*, and operates in a country that is a member of the FATF (see Appendix E) or a subsidiary of such a corporation whose financial statements are consolidated with the financial statements of publicly traded corporation.

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 4: OTHER CORPORATIONS AND ENTITIES

Requirement and Reference	Details
Information to be obtained PCMLTF Regs. 23(1), 57(3)	• Name • Address • Nature of principal business • Intended use of the account
If a corporation, management information to be obtained PCMLTF Reg. 11.1 (1)(a)	All directors • Name • Occupation
Beneficial ownership IIROC Rule 1300.1(b)(1); PCMLTF Reg. 11.1(1)(a) IIROC Rule 1300.1(b)(1) PCMLTF Reg. 11.1(1)(b)	Corporation - Individuals owning or controlling, directly or indirectly, more than 10% of the shares • Name • Address • Citizenship • Occupation • Employer Other entity - Individuals owning or controlling, directly or indirectly, more than 10% of the entity • Name • Address • Citizenship • Occupation • Employer
IIROC Rule 1300.1(e) PCMLTF Reg. 11.1(1)	Trust - Settlor and known beneficiaries of more than 10% • Name • Address • Citizenship • Occupation • Employer **Timing:** No later than the time of verification of the existence of the entity, i.e. within 30 days of account opening.
Exceptions to identification of beneficial owners IIROC Rules. 1300.1(c), (f)	• Publicly traded corporation • Affiliate of a publicly traded corporation • Publicly traded trust • Testamentary trust

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 4: OTHER CORPORATIONS AND ENTITIES

Requirement and Reference	Details
Exceptions to identification of beneficial owners under IIROC Rules not excepted under PCMLTF Regulation IIROC Rules 1300.1(c), (f) PCMLTF Reg. 11.1(1), 62(m), 62(n)	Publicly traded corporation • With less than net assets of $75 million on its last audited balance sheet, or • Whose shares are not traded on a Canadian stock exchange or a stock exchange designated under subsection 262(2) of the Income Tax Act (see Appendix F) and operates in a country that is a Member of FATF (see Appendix J) • Affiliate of any publicly traded corporation other than a subsidiary whose financial statements are consolidated with those of the parent company Publicly traded trust Testamentary trust
Identification of beneficial owners of the above IIROC exempt but not PCMLTF Reg. exempt entities PCMLTF Reg. 11.1(1)(a) PCMLTF Reg. 11.1(1)(b)	Corporation - Individuals owning or controlling, directly or indirectly, more than 25% of the shares • Name • Address • Occupation Other entity - Individuals owning or controlling, directly or indirectly, more than 25% of the entity • Name • Address • Occupation **Timing:** At the time of verification of the existence of the entity (i.e. within 30 days of account opening)
Signature document PCMLTF Reg. 23(1)(a)(i)	Signature card, account operating agreement or account application bearing the signature of the person authorized to give instructions for the account
If a corporation, other documents PCMLTF Reg. 31(1)(b)	Copy of the part of official corporate records that contains any provision relating to the power to bind the corporation in respect of the account (i.e. Corporate Resolution)

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 4: OTHER CORPORATIONS AND ENTITIES

Requirement and Reference	Details
Verification of the existence of the entity PCMLTF Regs. 57(3), 65(1) PCMLTF Regs. 57(4), 66(1) PCMLTF Regs. 65(2)(d), 66(2)(d) PCMLTF Regs. 65(3), 65(4), 66(3), 66(4)	Corporation • Certificate of corporate status • A record that it is required to file annually under the applicable provincial securities legislation, or • Any other record that ascertains its existence as a corporation. Other entity • Partnership agreement • Articles of association, or • Other similar record that ascertains its existence The record may be in paper form or in an electronic version that is obtained from a publicly accessible source. **Timing:** Within 30 days of account opening **Records required:** • Paper copy of record referred to, or • Electronic record o Registration number o Type of record referred to o Source of the electronic version of the record
Identity verification: Individuals authorized to give instructions PCMLTF Regs. 57(1), 62(a)	Verification of up to three individuals authorized to give instructions for the account **Process:** Methods described in Appendix A for individuals **Timing:** Before conducting any transactions other than an initial deposit **Records required:** Records described in Appendix A for individuals
Identity verification: Beneficial owners IIROC Regs. 1300.1(b)(ii), e(ii)	**Process:** Any method that enables the Dealer Member to form a reasonable belief that it knows the true identity of each individual **Timing:** As soon as practicable and in any event no later than 6 months after account opening

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 4: OTHER CORPORATIONS AND ENTITIES

Requirement and Reference	Details
Exemptions from information and identity verification requirements	• An account established pursuant to the escrow requirements of a Canadian securities regulator or Canadian stock exchange or any provincial legislation • In respect of which instructions are authorized to be given by a o financial entity o a securities dealer o life insurance company • A corporation that has minimum net assets of $75 million on its last audited balance sheet and whose shares are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the Income Tax Act (see Appendix F), and operates in a country that is a member of the FATF (see Appendix E) • A subsidiary of the above whose financial statements are consolidated with the financial statements of publicly traded corporation • A public body • Any department or agent of Her Majesty in right of Canada or of a province • An incorporated city, town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body or an agent of any of them • An organization that operates a public hospital and that is designated by the Minister of National Revenue as a hospital authority under the Excise Tax Act, or any agent of such an organization. • A subsidiary of a public body whose financial statements are consolidated with the public body
Third party information PCMLTF Regs. 9(1), 9(2),	Records of individual third party required • Name • Address • Date of birth • Principal business or occupation • Relationship between the individual and the third party Records of entity third party required • Name • Address • Nature of principal business • If a corporation, incorporation number and place of issue • Relationship between the individual and the entity
Large cash transaction reports	Same requirements as in Appendix A

APPENDIX A: SUMMARY OF CUSTOMER DUE DILIGENCE AND LARGE CASH TRANSACTION REQUIREMENTS

TABLE 4: OTHER CORPORATIONS AND ENTITIES

Requirement and Reference	Details
Exemption from large cash transaction reports	A public body • any department or agent of Her Majesty in right of Canada or of a province • an incorporated city, town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body or an agent of any of them An organization that operates a public hospital and that is designated by the Minister of National Revenue as a hospital authority under the *Excise Tax Act*, or any agent of such an organization

APPENDIX B: SUMMARY OF PCMLTFA, PCMLTF REGULATIONS AND IIROC RULES APPLICABLE TO DEALER MEMBERS

Description	PCMLTFA Section(s)	PCMLTF Regulation Section(s)	IIROC Rule
Compliance program requirements	9.6(1)	71	
Customer account records	6	23	
Exceptions to record keeping and identity verification requirements	6, 6.1	62, 63	1300.1(c), (d), (f)
Identification of politically exposed foreign persons	9.3(1)	57.1	
Information requirements regarding corporations and other entities, including beneficial owners	6	11	1300.1(b), (e), (h), (l)
Large cash transaction and electronic funds transfer reports and records	6, 9(1)	21-22	
Non face-to-face verification methods	6.1	Schedule 7	
Prohibition against dealing with shell banks			1300.1(i), (j), (k)
Prohibition against opening accounts if information cannot be obtained or identity verified	9.2		1300.1(g)
Record keeping requirements	6	67, 69, 70	
Risk assessment and measures for high-risk accounts or business.	9.6	71.1	
Special procedures for accounts of politically exposed foreign persons	9(3)(2)	23(1)(f) 67.1	
Third party interest in accounts	6	9	
Third party transactions	6	8	
Use of agents or mandataries to verify identity	6.1	64.1	
Verification methods – corporations and other entities	6.1	65, 66	
Verification methods - individuals	6.1	64	
Verification methods for corporations and other entities	6	65-66	
Verification of identity	6.1	53, 53.1, 57	1300.1(b)
Verification of the identity of beneficial owners			1300.1(b), (e), (h), (l)
Verification records	6.1	67, 68, 69, 70	1300.1(n)

Appendix C: Penalties for Violations of PCMLTFA

Requirement Violated	PCMLTFA Section	Maximum Penalty	
		Conviction on Indictment	**Summary Conviction**
Maintenance of records as prescribed in the regulations	6	$500,000 fine or five years imprisonment or both	$50,000 fine or six months imprisonment or both
Verification of identity as prescribed in the regulations	6.1		
Reporting to FINTRAC under other Acts of Parliament or regulations	9.1		
Prohibition against opening an account if unable to establish the client's identity	9.2		
Determination regarding whether a client is a politically exposed foreign person	9.3		
Inclusion of client information on electronic funds transfers	9.5		
Establishment of an anti-money laundering compliance program including risk assessments and special measures regarding high-risk activities	9.6		
Reporting of export and import of currency and monetary instruments	12		
Reporting to FINTRAC of suspicious transactions and attempted suspicious transactions	7	$2,000,000 fine or 5 years imprisonment or both	$500,000 fine or six months imprisonment or both on first offence; $1,000,000 fine or one year imprisonment or both on a subsequent offence
Reporting to FINTRAC of disclosures regarding terrorist property that are required under the *Criminal Code* and *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*	7.1		
Prohibition against disclosing the making or contents of a suspicious transaction report "with the intent to prejudice a criminal investigation"	8	Two years imprisonment	N/A
Reporting of transactions prescribed in the regulations – i.e. large cash transaction reports	9	N/A	$500,000 fine on first offence; $1,000,000 fine for each subsequent offence

APPENDIX D: CLASSIFICATION OF VIOLATIONS FOR DETERMINING ADMINISTRATIVE PENALTIES

VERY SERIOUS VIOLATIONS		
Requirement Description	**Source**	**Section**
Inclusion of required information in a suspicious transaction report (STR)	STR Regulations	9(1)
Send a STR without delay		10

SERIOUS VIOLATIONS		
Requirement Description	**Source**	**Section**
Ensure the development and application policies and procedures consistent with the requirements of PCMLTFA regarding record keeping, identity verification procedures and implementation of a compliance regime in wholly-owned subsidiaries and branches outside of Canada	PCMLTFA	9.7(1) 9.8
Give reasonable assistance and information reasonably required in a FINTRAC compliance review or provide documents required for the review.		62(2), 63.1(2)
Appoint a person responsible for the implementation of an AML/CFT compliance program	PCMLTFA Regulations	71(1)(a)
Develop and apply compliance policies and procedures that are kept up-to-date and approved by a senior officer		71(1)(b)
Assess and document AML/CFT risk		71(1)(c)
Develop and maintain a written AML/CFT training program		71(1)(d)
Institute and document an biennial review and testing of the compliance program and provide a written report to a senior officer including the findings, any updates made to the policies and procedures during the period under review and the status of implementation of the updates		71(1)(e) 71(2)
Take reasonable measures regarding high risk accounts including measures to keep client information up to date, conduct ongoing monitoring for suspicious transactions and mitigate the risks		71.1
Send a STR within 30 days of detecting a fact that gives reasonably grounds to believe that the transaction or attempted transaction is suspicious	STR Regulations	9(2)
Send a STR electronically if the Dealer Member has capability of doing so	STR Regulations	12(1)
Send a paper STR in accordance with FINTRAC guidelines		12(2)
Send a terrorist property report in accordance with FINTRAC guidelines		12(3)

Appendix D: Classification of Violations for Determining Administrative Penalties

MINOR VIOLATIONS		
Requirement Description	**Source**	**Section**
Keep a record of a policy or procedure that should otherwise have been developed for a wholly-owned subsidiary but contravene the laws of the country in which it is located	PCMLTFA	9.7(2)
Convert foreign currency transactions into Canadian dollars based on rates prescribed in the section	PCMLTFA Regulations	2
Send reports under the PCMLTFA Regulations to FINTRAC electronically if the Dealer Member has the capability of doing so		4(1)
Send a paper report under the PCMLTFA Regulations in the prescribed format		4(2)
Report an electronic funds transfer within 5 working days after the transfer		5(1)
Rake reasonable measures to ascertain whether an individual giving cash is acting on behalf of a third party or to record information regarding third parties or suspected third parties		8(1)-(3)
Take reasonable measures when opening and account whether it will be used by or behalf of a third party or to record information regarding third parties or suspected third parties		9(1)-(3)
Take reasonable measures to obtain required information regarding the directors of corporations and beneficial owners of corporations and other entities and record the information obtained or the reason it could not be obtained		11.1(1)-(2)
Determine whether a not-for-profit organization is a registered charity or, if not, it solicits donations from the public		11.1(3)
File a large cash transaction report and maintain a large cash transaction record		21-22
Keep required records regarding new accounts		23
Verify identity of those authorized to give instructions in an account in the required manner and within the required period		57(1)
Confirm the existence of a corporation or other entity in the required manner within the required period		57(3), 57(4)
Take reasonable measures to determine whether a new client is a politically exposed foreign person		57.1(2)
Take reasonable measures within the prescribed period to determine whether an existing client is a politically exposed foreign person		57.1(2)

Appendix D: Classification of Violations for Determining Administrative Penalties

MINOR VIOLATIONS - Continued		
Requirement Description	**Source**	**Section**
Enter into an agreement with and obtain the required information from an agent or mandatary relied upon to verify client identity	PCMLTFA Regulations	64(1)(2)
Keep copies of records relied upon to confirm the existence of corporations and other entities		65(3)-(4) 66(3)-(4)
Include required information in an electronic funds transfer send and take reasonable measure to ensure that it is included in electronic funds transfers received		66.1(1)-(2)
Keep records regarding identity verification		67
Establish source of funds, obtain senior management approval and conduct enhanced monitoring of accounts of politically exposed foreign persons		67.1
Maintain records for five years in a manner such that they can be provided to an authorized person within 30 days of a request		69(1)-70
Keep a copy of a STR for five years	STR Regulations	12.1-12.3

APPENDIX E: MEMBERS OF FATF (FINANCIAL ACTION TASK FORCE)

1. Argentina
2. Australia
3. Austria
4. Belgium
5. Brazil
6. Canada
7. China
8. Denmark
9. European Commission
10. Finland
11. France
12. Germany
13. Greece
14. Gulf Co-operation Council*
15. Hong Kong, China
16. Iceland
17. India
18. Ireland
19. Italy
20. Japan
21. Kingdom of the Netherlands**
22. Luxembourg
23. Mexico
24. New Zealand
25. Norway
26. Portugal
27. Republic of Korea
28. Russian Federation
29. Singapore
30. South Africa
31. Spain
32. Sweden
33. Switzerland
34. Turkey
35. United Kingdom
36. United States

* The individual members of the Gulf Co-operative Council - Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates – are not members of FATF.

** The Kingdom of the Netherlands: the Netherlands, the Netherlands Antilles and Aruba.

APPENDIX F: STOCK EXCHANGES RECOGNIZED UNDER SECTION 262(1) OF THE *INCOME TAX ACT* IN FATF MEMBER COUNTRIES)

Australia:	Australian Securities Exchange
Austria:	Vienna Stock Exchange
Belgium:	Euronext Brussels
Canada:	Canadian National Stock Exchange (CNSX)
	Montreal Exchange
	TSX Venture Exchange (Tiers 1 and 2)
	Toronto Stock Exchange
Denmark:	Copenhagen Stock Exchange
Finland:	Helsinki Stock Exchange
France:	Euronext Paris
Germany:	Frankfurt Stock Exchange
Hong Kong:	The Hong Kong Stock Exchange
Ireland:	Irish Stock Exchange
Israel:	Tel Aviv Stock Exchange
Italy:	Milan Stock Exchange
Japan:	Tokyo Stock Exchange
Luxembourg:	Luxembourg Stock Exchange
Mexico:	Mexico City Stock Exchange
Netherlands:	Euronext Amsterdam
New Zealand:	New Zealand Stock Exchange
Norway:	Oslo Stock Exchange
Poland:	The main and parallel markets of the Warsaw Stock Exchange
Singapore:	Singapore Stock Exchange
South Africa:	Johannesburg Stock Exchange
Spain:	Madrid Stock Exchange
Sweden:	Stockholm Stock Exchange
Switzerland:	SWX Swiss Exchange
United Kingdom:	London Stock Exchange
United States:	American Stock Exchange
	Boston Stock Exchange
	Chicago Board of Options
	Chicago Board of Trade
	Chicago Stock Exchange
	National Association of Securities Dealers Automated Quotation System
	National Stock Exchange
	New York Stock Exchange
	NYSE Arca
	Philadelphia Stock Exchange

APPENDIX G: REFERENCE MATERIAL

Laws and Regulations

Cross-border Currency and Monetary Instruments Reporting Regulations	http://laws.justice.gc.ca/PDF/Regulation/S/SOR-2002-412.pdf
IIROC Rule 1300	http://iiroc.knotia.ca/Knowledge/View/Document.cfm?Ktype=445&linkType=toc&dbID=201002341&tocID=631
Proceeds of Crime (Money Laundering) and Terrorist Financing Act	http://laws.justice.gc.ca/PDF/Regulation/S/SOR-2002-184.pdf
Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations	http://laws.justice.gc.ca/PDF/Regulation/S/SOR-2007-292.pdf
Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations	http://laws.justice.gc.ca/PDF/Regulation/S/SOR-2002-184.pdf
Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations	http://laws.justice.gc.ca/PDF/Regulation/S/SOR-2001-317.pdf

Financial Action Task Force Recommendations

FATF 40 Recommendations on money laundering	http://www.fatf-gafi.org/dataoecd/7/40/34849567.PDF
FATF 9 Special Recommendations on terrorist financing	http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf

Guidance

FATF Money Laundering FAQ	http://www.fatf-gafi.org/document/29/0,3343,en_32250379_32235720_33659613_1_1_1_1,00.html
FATF: "Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing," June, 2007	http://www.fatf-gafi.org/dataoecd/43/46/38960576.pdf
FATF: "Money Laundering and Terrorist Financing in the Securities Sector," October, 2009	http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf
FINTRAC Guidelines including a general background on money laundering and terrorist financing, suspicious transactions, terrorist property reports and Large Cash Transaction Reports can be obtained through links	http://www.fintrac-canafe.gc.ca/publications/guide/guide-eng.asp.
FINTRAC Information for Securities Dealers containing a high level outline of requirements	http://www.fintrac-canafe.gc.ca/re-ed/sec-eng.asp
Joint Money Laundering Steering Group, UK: "Prevention of money laundering / combating the financing of terrorist: Guidance for the UK Financial Sector, Part II: Sectoral Guidance," January, 2006	http://www.jmlsg.org.uk/content/1/c6/01/09/68/Part_II_2006__inc_CU.pdf
Joint Money Laundering Steering Group, UK: Prevention of money laundering / combating the financing of terrorist: Guidance for the UK Financial Sector, Part I," January, 2006	http://www.jmlsg.org.uk/content/1/c4/98/00/Final_Part_I_030306.pdf
OSFI Guideline B-8	http://www.osfi-bsif.ca

Wolfsberg Group: "Wolfsberg Statement on AML Screening, Monitoring and Searching 2009,", November 9, 2009	http://www.wolfsberg-principles.com/pdf/Wolfsberg_Monitoring_Screening_Searching_Paper-Nov_9_2009.pdf

Typologies

Council of Europe Committee of experts on the evaluation of anti-money laundering measures and the financing of terrorism (MONEYVAL): "Use of securities in money laundering schemes," July, 2008	http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2008)24Reptyp_securities.pdf
Egmont Group: "FIU's in action: 100 cases from the Egmont Group"	http://www.egmontgroup.org/
FATF: "Money Laundering and Terrorist Financing in the Securities Sector," October, 2009	http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf

Country Evaluations

Asia/Pacific Group on Money Laundering Mutual Evaluation Reports Round 1 (2000-2005)	http://www.apgml.org/documents/default.aspx?DocumentCategoryID=8
Asia/Pacific Group on Money Laundering Mutual Evaluation Reports Round 1 (2000-2005)	http://www.apgml.org/documents/default.aspx?DocumentCategoryID=17
Caribbean Financial Action Task Force Mutual Evaluation Reports	http://www.cfatf-gafic.org/index.php
Council of Europe Committee of experts on the evaluation of anti-money laundering measures and the financing of terrorism (MONEYVAL) Evaluation Reports	http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/Evaluation_reports_en.asp
Eastern and Southern Africa Anti-Money Laundering Group Mutual Evaluations	http://www.esaamlg.org/reports/me.php
Eurasian Group Mutual Evaluation Reports	http://www.eurasiangroup.org/en/mers.html
FATF Mutual Evaluations Reports	http://www.fatf-gafi.org/document/32/0,3343,en_32250379_32236982_35128416_1_1_1_1,00.html
Financial Action Task Force on Money Laundering in South America (GAFISUD) Evaluations (Spanish only)	http://www.gafisud.info/actividades.asp?offset=0
Inter Governmental Action Group Against Money Laundering in West Africa Mutual Evaluations	http://www.giaba.org/index.php?type=c&id=24&mod=2&men=2
Middle East and North Africa Financial Action Task Force Mutual Evaluations	http://www.menafatf.org/TopicList.asp?cType=train
Transparency International Corruption Perceptions Index	http://www.transparency.org/policy_research/surveys_indices/cpi/2009