

IIROC NOTICE

Rules Notice Guidance Note

Dealer Member Rules

Please distribute internally to:

Institutional
Internal Audit
Legal and Compliance
Retail
Senior Management
Trading Desk

Contact:

Madeleine A. Cooper
Policy Counsel, Member Regulation Policy
Telephone: 416.646.7203
e-mail: mcooper@iiroc.ca

David Wright
Senior Counsel, Business Conduct Compliance
Telephone: 416.943.6891
e-mail: dwright@iiroc.ca

GN-3200-20-003
####, 201#

Anti-Money Laundering Compliance Guidance

Executive Summary

Dealer Members (**Dealers**) are required to meet a variety of applicable rules relating to anti-money laundering (**AML**) and anti-terrorist financing (**ATF**), including:

- IIROC Rules,
- Canadian federal legislation,
- National Instrument 31-103 - Registration Requirements, Exemptions and Ongoing Registrant Obligations (NI 31-103), and
- other AML/ATF requirements applicable to Dealers for activities carried out in various jurisdictions.



Dealers must comply with all applicable laws and regulations relating to AML and ATF. We are publishing this Guidance to focus on the relationship between federal AML/ATF laws and IIROC client due diligence requirements to assist our Dealers in meeting their regulatory obligations.

This Guidance is effective on **June 1, 2020**.



Table of Contents

1. Introduction	5
1.1 Purpose.....	5
1.2 Scope	5
1.3 Responsibility for AML/ATF compliance reviews	5
2. Requirements.....	5
3. Compliance and Supervision programs	6
3.1 Designation of an AML compliance officer	6
3.1.1 Enterprise AML/ATF departments.....	7
3.2 Anti-money laundering policies and procedures	7
3.2.1 Client account forms.....	7
3.3 Enterprise risk assessment.....	7
3.4 Training.....	8
3.4.1 Minimum requirements.....	8
3.4.2 Keeping training current	8
3.4.3 Keeping training current	8
3.5 Review program	9
4. Client due diligence.....	9
4.1 Client due diligence requirements.....	9
4.2 Keeping client information current.....	10
4.3 Business Relationship Records	10
4.3.1 Business Relationships	10
4.3.2 Documentation	10
4.3.3 Periodic updating.....	11
4.3.4 Client risk assessment.....	11
4.4 Introducing and Carrying Brokers' obligations	12
4.5 Registered plan accounts	13
4.6 Trading authorization	13
4.7 Non-individual clients.....	13
4.7.1 Client structure	14
4.7.2 Direct or indirect control	14
4.7.3 Establishing identity.....	15
4.7.4 Identity verification timing	15
4.7.5 Exceptions to client identification requirements	16
4.7.6 Politically Exposed Persons and Heads of International Organizations	16



5.	Key risk indicators for Dealers	17
5.1	Client due diligence risks.....	17
5.1.1	Clients with complex ownership structures	17
5.1.2	Using accounts for undeclared purposes	18
5.2	Trading risks	18
5.2.1	Over-the-Counter (OTC) securities	18
5.2.2	Stock manipulation	18
5.2.3	Low-priced securities	18
5.2.4	Inactive issuers and shell companies.....	18
5.3	Non-trading risks	19
5.3.1	Cash deposits or withdrawals	19
5.3.2	Physical certificates deposits	19
5.3.3	Early redemption of securities.....	19
5.3.4	Requesting proceeds in the form of negotiable instruments	19
5.3.5	Transfer of funds between accounts	19
6.	Suspicious transactions.....	19
6.1	Account Supervision requirements.....	20
6.2	Account Supervision programs and ongoing monitoring	21
6.3	Enhanced measures for high risk business relationships	22
6.4	Other Compliance and Supervision systems and procedures	22
7.	U.N. suppression of terrorism reports and similar requirements.....	22
8.	Applicable Rules.....	22
9.	Previous Guidance Notes.....	22
10.	Appendices.....	23
	Appendix A: Client Due Diligence and Large Cash Transaction Requirements	24
	Appendix B: More Information on Money Laundering Legislation	25
	Appendix C: Penalties for Violations of PCMLTFA	28
	Appendix D: Classification of Violations for Determining Administrative Penalties	29
	Appendix E: Members of FATF (Financial Action Task Force)	30
	Appendix F: Stock Exchanges Recognized Under Section 262(1) of the <i>Income Tax Act</i> in FATF Member Countries	31
	Appendix G: Reference Material.....	32
	Appendix H: Client Identification and Verification Requirements Comparison Chart	33
	Appendix I: Beneficial Ownership Diagram	35



1. Introduction

1.1 Purpose

In this Guidance, we outline the AML/ATF regulatory requirements and expectations applicable to Dealers. We also include links to resources to assist Dealers in meeting their obligations.

1.2 Scope

Dealers have a variety of business models. We do not discuss each type in this Guidance. We expect each Dealer will adapt its AML/ATF compliance program(s) to its business model.

1.3 Responsibility for AML/ATF compliance reviews

Regulatory oversight of Dealer compliance with AML/ATF rules is shared between IIROC and the Financial Transactions and Reports Analysis Centre of Canada¹ (**FINTRAC**). FINTRAC includes IIROC member firms in its AML examination coverage, outreach and guidance. IIROC's Business Conduct Compliance unit also performs focused AML/ATF testing as part of regularly scheduled examinations of Dealers, based on an analysis of various risk-based factors. IIROC and FINTRAC exchange information pertaining to Dealer AML/ATF compliance on a regular basis (through an information sharing agreement). Even in cases where IIROC does not perform focused AML/ATF testing as part of a Dealer exam, we will generally review certain aspects of the Dealer's AML/ATF compliance program as part of other testing including with respect to client identification, trading activity, and fund transfers.

2. Requirements

IIROC client due diligence requirements² have purposes that differ from, and are in addition, to AML/ATF requirements. Some of our client due diligence rules require more information than the related [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Act \(PCMLTFA\)](#) or [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Regulations \(PCMLTF Regulations\)](#) provisions to ensure that Dealers obtain information necessary to investigate capital markets abuse.

We remind Dealers that where IIROC requirements differ from applicable laws, they must comply with the more stringent requirement. In this Guidance, we refer to the PCMLTFA and the PCMLTF Regulations jointly as the **AML rules**.

IIROC has its own client identification requirements³ applicable to all Dealers. These requirements are primarily set out in Part A of IIROC Rule 3200.

Dealers may also be subject to certain client due diligence requirements under National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations (NI-31-103)*.

¹ FINTRAC administers PCMLTFA and associated regulations.

² See Part A of IIROC Rule 3200, specifically section 3202.

³ See Part A of IIROC Rule 3200, specifically sections 3203 through to 3207.



3. Compliance and Supervision programs

Under the PCMLTFA, Dealers must establish an AML/ATF compliance program. The PCMLTF Regulations set out specific requirements, including:

- the appointment of a person responsible for the compliance program,
- the development and application of compliance policies and procedures that are 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, and implementation of measures to mitigate high-risk scenarios,
- an ongoing written compliance training program for employees⁴ of the firm, and
- a review of policies and procedures to test their effectiveness to be conducted every two years by an internal or external auditor.

Under IIROC Rules 1400 and 3900, Dealers are required to establish a compliance and supervision program. A Dealer's AML compliance program could be a part of its compliance and supervision program.

FINTRAC's [Compliance program requirements](#) guidance contains details on specific AML requirements for compliance programs.

3.1 Designation of an AML compliance officer

A Dealer must designate a person responsible for its anti-money laundering program (**AML Compliance Officer**)⁵.

Based on the roles and responsibilities of the Chief Compliance Officer (**CCO**) set out in IIROC Rule 3900, a CCO could be appointed as the AML Compliance Officer responsible for the AML/ATF compliance program, including approving policies and procedures. While this could help the CCO ensure integration of AML/ATF procedures into the firm's compliance program, Dealers may want to assess their CCO's duties first to determine whether they have the capacity to fulfill this additional function.

Dealers' AML Compliance Officers should remain up-to-date with AML/ATF rules and risks. If CCOs deal with day-to-day regulatory issues, changes to securities regulations and to AML/ATF requirements, they may not have enough time to maintain the knowledge needed to oversee an effective AML/ATF regime. If this is the case, the Dealer may want to consider designating a different qualified individual as the AML Compliance Officer.

⁴ Where the term "employee" is used with reference to Dealers, it includes Registered Representatives in a principal/agent relationship with a Dealer Member and any employees of an agent who are engaged in the Dealer Member's business.

⁵ See section 71 of the PCTFML Regulations.



3.1.1 Enterprise AML/ATF departments

Some Dealers maintain enterprise AML/ATF departments across the Dealer and its affiliates. As set out above, these Dealers must designate an AML Compliance Officer; however, that person can report to both the enterprise group and senior management of the Dealer. The Dealer remains responsible for its own AML/ATF program and cannot delegate this responsibility to an enterprise group. Dealer senior management must be kept informed of significant issues. In addition, where the AML rules require approval of a senior officer, it should be the Dealer's senior officer.

For further guidance on the appointment of an AML Compliance Officer, Dealers can consult FINTRAC's [Compliance program requirements](#) guidance.

3.2 Anti-money laundering policies and procedures

A Dealer's AML/ATF program should include systems and controls designed to prevent and detect money laundering and terrorist financing and to comply with applicable laws.

Dealers can combine their policies and procedures for compliance with AML/ATF rules with other requirements pertaining to securities laws and IIROC requirements. However, Dealers should not rely solely on systems and procedures designed to prevent money laundering and terrorist financing to meet securities requirements, such as suitability.

As a best practice, Dealers should integrate AML/ATF policies and procedures with other compliance and supervisory procedures. This will ensure AML/ATF compliance is a part of the business and will not be duplicative. While learning materials outlining specific AML/ATF procedures are a useful part of an education process, integration into the firm's overall know-your-client (**KYC**), compliance and supervisory procedures ensure that they become part of the established practice.

Dealers should review their AML/ATF procedures regularly and update them as needed based on any legal/regulatory or business/operational changes.

Dealers may want to consult FINTRAC's [Compliance program requirements](#) guidance for more details on AML/ATF compliance policies and procedures.

3.2.1 Client account forms

As a best practice, Dealers should address AML/ATF client information requirements in their new account forms and related documents. To assist clients in accurately completing their forms, Dealers should include definitions where appropriate. For example, a question on an application regarding who is a politically exposed person or head of an international organization should have a definition of those terms, especially if clients complete the form.

3.3 Enterprise risk assessment

Dealers must conduct a money laundering/terrorist financing risk assessment of their business. Section 71 of the PCMLTF Regulations lists the minimum factors to consider in assessing this risk:

- clients and business relationships,



- products and delivery channels,
- geographic location of activities,
- impact of new technologies on clients and business activities,
- risks of an affiliate, and
- other relevant factors.

FINTRAC has many tools to assist Dealers in conducting risk assessments. Dealers may want to consult the following when establishing and conducting risk assessments:

- [Risk-based approach workbook for securities dealers](#),
- [Guidance on the Risk-Based Approach to Combatting Money Laundering and Terrorist Financing](#), and
- [Compliance program requirements](#).

3.4 Training

Dealers must train all employees with respect to AML/ATF procedures, including the detection of attempted and/or completed suspicious transactions and compliance with AML rules and IIROC requirements.

3.4.1 Minimum requirements

Dealers should tailor the contents of this AML/ATF training to reflect their business model. They should address at minimum:

- the Dealer's KYC policy and procedures,
- the roles of client-facing Approved Persons, operations, Supervisors, management and others,
- potential indicators of suspicious activity,
- rules and regulations for reporting currency transactions (if applicable) and suspicious transactions,
- Dealer procedures for reporting unusual transactions and reporting suspicious transactions, and
- civil and criminal penalties associated with money laundering and terrorist financing.

Dealers should also maintain a record of all individuals who participated in the training.

3.4.2 Keeping training current

Dealers should update their training materials to reflect any developments, new techniques or money laundering trends identified by various government agencies such as FINTRAC and the Financial Action Task Force (**FATF**).

3.4.3 Tailoring Training

Dealers should consider tailoring their training for different roles within the firm. For example, while Approved Persons with direct client contact may be in the best position to identify suspicious activity,



other departments such as treasury, operations, margin, credit, corporate security, audit, legal and compliance should be able to identify red flags for their areas of activity.

3.5 Review program

Under the PCMLTF Regulations, a Dealer's internal or external auditors must conduct a compliance effectiveness review of the Dealer's AML program at least once every two years. At a minimum, the review must cover the topics discussed in sections 3.2, 3.3 and 3.4.

Following this review, Dealers must report in writing the following to senior management:

- their findings, including any deficiencies identified, planned corrective actions, and implementation timelines, and
- any policies and procedure updates and their implementation status.

Dealers should include this report (or a summary of it) in the CCO's annual report to the Board on compliance matters.⁶

4. Client due diligence

4.1 Client due diligence requirements

The PCMLTF Regulations establish specific "client due diligence" (**CDD**) requirements, which include information gathering, client identity verification and record keeping. IIROC Rules 3100, 3200 and 3400 contain similar requirements, including KYC and client identification rules. We expect Dealers will leverage the same client information to satisfy their obligations under both the IIROC Rules and the PCMLTF Regulations.

The IIROC Rules and the PCMLTF Regulations sometimes require Dealers to look at client information from different perspectives and consider different or additional elements. The purpose of the PCMLTFA is to detect and deter money laundering and terrorist financing. IIROC's primary mandate is to protect investors and support healthy capital markets. These different objectives may result in inconsistencies between the two sets of requirements. Dealers should be aware of these different objectives when collecting CDD information.

For example, under the AML rules, Dealers are required to collect information on the purpose and intended nature of a business relationship (as discussed further in section 4.3 of this Guidance). The objective of collecting this information is to detect if any client transactions are suspicious and could indicate money laundering or terrorist financing. The IIROC Rules require Dealers to collect their client's investment objectives to ensure the investments in their clients' accounts are suitable for them. A Dealer may collect the same information under both requirements, but may not be using it for the same purpose.

⁶ As required by IIROC Rule sub-section 3915(1).



4.2 Keeping client information current

The PCMLTF Regulations and the IIROC Rules require Dealers keep CDD and KYC information up to date. Sub-section 3202(3) of the IIROC Rules requires a Dealer to take reasonable steps to keep client identification information current. Dealers should update this information any time there is a material change in the client's circumstances.

We recommend the following best practices⁷:

- for full-service Dealers, instruct Approved Persons to update client information as necessary during their regular meetings with clients, and advise clients in account opening documentation that they have an obligation to notify their Approved Person when there is a material change in their circumstances, and
- use these client touchpoints to help meet AML rule requirements.

For clients who are not individuals, FINTRAC recommends firms keep their information current by consulting paper or electronic records or verbally obtaining information. FINTRAC also recommends that, for individuals, a firm update the client's information using options available to identify individuals who are not physically present (i.e., either using a Dealer's affiliate or co-member or a combination of methods).⁸ Dealers can also use this information to help meet their obligations under our rules.

4.3 Business Relationship Records

4.3.1 Business Relationships

Under the PCMLTF Regulations, firms must establish and maintain records relating to business relationships (**Business Relationship Record**), in addition to basic client identification requirements. A business relationship exists when:

- a client holds one or more accounts with a Dealer, or
- a client conducts two or more transactions within a five-year period that require the Dealer to ascertain the identity of the client.

If a client maintains multiple accounts with a Dealer associated with various products and services, the Dealer should consider the business relationship as a whole when conducting the risk assessment and resulting monitoring.

4.3.2 Documentation

Dealers must document the purpose and intended nature of each business relationship. They should include the client's intentions for the assets held within its account(s).

⁷ See [IIROC Notice 12-0109 Know your client and suitability](#).

⁸ See FINTRAC guidance [When to identify individuals and confirm the existence of entities – Securities dealers](#)



Dealers may use the client's investment objectives to inform the purpose and intended nature of the business relationship. For business relationships involving multiple accounts, the Dealer must include all accounts when documenting the purpose and intended nature of the business relationship.

4.3.3 Periodic updating

Dealers must keep the Business Relationship Record current. The Business Relationship Record helps Dealers anticipate client activities. Through ongoing monitoring, Dealers may notice a deviation from anticipated client activity triggering them to reassess the client's risk level. Dealers may also need to reassess the client's KYC and/or the suitability of its overall portfolio.

As noted in section 4.2, Dealers can update client information during their periodic meetings with clients. If the client's beneficial ownership has changed, the Dealer must determine who owns or controls the entity by complying with Part A of IIROC Rule 3200 and section 11.1 of the PCMLTF Regulations⁹. The Dealer must record the information obtained to update the client's beneficial ownership information.

Dealers must review high risk business relationships more frequently. Dealers should determine the frequency of the review based on their risk assessment. Dealers should document the high risk nature of the business relationship in their risk assessment.

4.3.4 Client risk assessment

Dealers must conduct a risk assessment for all clients. In certain cases, a business relationship may exist even if the client has not opened an account. For example, an investment banking relationship does not necessarily involve opening a client account. In this case, the Dealer may not be required to ascertain identity under the AML rules nor document or monitor the business relationship. However, the Dealer must still conduct a risk assessment based on a number of factors:

- the products, services and channels¹⁰ the client uses,
- where the client lives or which countries they transact in, and
- the client's characteristics, activities and transaction patterns.

Dealers should use the information contained in the Business Relationship Record to identify risk factors that apply to the overall business relationship.

For more information on the PCMLTF Regulations' client due diligence and business relationship requirements, including ongoing monitoring and risk assessments, please consult the following FINTRAC Guidance:

- [Business relationship requirements](#),
- [When to identify individuals and confirm the existence of entities – Securities dealers](#),

⁹ As described in [Notice 19-0145](#), Part A of IIROC Rule 3200 was recently amended to materially conform with section 11.1 of the PCMLTF Regulations.

¹⁰ As discussed in FINTRAC's Compliance program requirements guidance.



- [Methods to identify individuals and confirm the existence of entities, and](#)
- [Compliance program requirements.](#)

4.4 Introducing and Carrying Brokers' obligations

PCMLTF Regulations exempt carrying brokers from CDD for clients of introducing brokers whose accounts they carry¹¹. Introducing brokers are responsible for conducting CDD. The PCMLTF Regulations are silent on introducing broker/carrying broker arrangement types, so this exception applies to all types of arrangements. However, this exception covers only the PCMLTF Regulations' CDD requirements; it does not cover large cash transactions and suspicious transactions reporting requirements.

Regardless of this exception, under the IIROC Rules, we consider a client to be a client of both the introducing and the carrying broker in all types of arrangements.

As a best practice, we recommend introducing and carrying brokers address AML/ATF compliance in their introducing broker/carrying broker agreements. At minimum, these agreements should address the following:

- which party is responsible for anti-money laundering procedures,
- the information the introducing firm needs to conduct CDD in the case the carrying broker provides standard account documentation forms,
- reports the carrying broker will provide to the introducing broker to fulfill its transaction monitoring responsibilities,
- what support the carrying broker will provide, such as checking of client names against terrorist lists,
- compliance with record keeping and access requirements, and
- if clients can deal directly with the carrying firm to conduct transactions such as deposits, withdrawals and wire transfers, there should be communication between the firms to enable proper monitoring for unusual activity.

Carrying brokers may decide to develop or enhance tools to assist introducing brokers in analyzing client transactions. These tools could include client account deposit and trade reports. Carrying brokers should disclose these reports to introducing brokers at the inception of the introducing/carrying relationship.

Introducing and carrying brokers should communicate effectively when dealing with indications of unusual activity. For example, when a carrying broker reports a potentially suspicious activity to an introducing broker, the introducing broker should show the carrying broker how that activity has been addressed. Introducing brokers can advise their carrying broker of other activity that should be reviewed.

¹¹ See the PCMLTF Regulations section 62(2)(o).



Introducing and carrying brokers should advise anyone conducting an audit of their anti-money laundering procedures of their agreed responsibilities. Both Dealers' auditors should work together and share information to ensure both parties are executing their responsibilities according to applicable laws and requirements and the introducing/carrying broker agreement.

4.5 Registered plan accounts

The PCMLTF Regulations exempt registered plan accounts, such as locked-in retirement plan accounts and registered retirement savings plan accounts from the following requirements¹²:

- client due diligence, including politically exposed persons and heads of international organizations requirements, under [s.57 and s.57.1 of the PCMLTF Regulations](#), and
- client account record keeping under [s.23 of the PCMLTF Regulations](#).

The IIROC Rules do not include equivalent exemptions for registered plan accounts because our requirements have a different purpose. Dealers must comply with Part A of IIROC Rule 3200 when opening all client accounts, including registered plan accounts. Dealers must establish the identity of every client who opens a registered plan account using such methods that allow them to form a reasonable belief it knows the identity of the individual and by taking reasonable measure to confirm the information obtained. As a best practice, Dealers should use the same methods to verify the identity of registered plan owners as they use for all other clients.

While Dealers must comply with Part A of IIROC Rule 3200 when opening registered plan accounts, they are not required to comply with the PCMLTF Regulations those accounts are exempted from, including the politically exposed persons and heads of international organizations requirements.

4.6 Trading authorization

Subsection 3220(4) of the IIROC Rules requires Dealers to record all individuals who have trading authorization over their clients' accounts.

Under [s.23 of the PCMLTF Regulations](#), Dealers must record (amongst other items) the signature of every person authorized to give instructions on the account. [Subsection 57\(1\) of the PCMLTF Regulations](#) requires Dealers ascertain the identity of every person who can give instructions with respect to an account.

Dealers can use the information they collect under these PCMLTF Regulations on individuals authorized to give instructions to comply with subsection 3220(4) of the IIROC Rules.

4.7 Non-individual clients

As discussed in section 5.1.1, money launderers can use corporations and other non-individual accounts to shield their identity and make it more difficult to investigate their illegal conduct.

¹² See PCMLTF Regulations, [s.62\(2\)\(i\)](#)



Part A of IIROC Rule 3200 was initially implemented to deter money laundering through such entities and to assist in market conduct investigations. While the IIROC Rules are intended to be consistent with similar provisions in National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations* and with the PCMLTF Regulations, in certain respects, the IIROC Rules may still be more stringent than the PCMLTF Regulations.¹³ Dealers must always comply with the strictest requirement.

4.7.1 Client structure

IIROC Rule 3200 requires Dealers to establish the identity¹⁴ of any individual who exercises control over any corporations, partnerships and trusts who are their client, in addition to these clients' beneficial owners, beneficiaries and other controlling individuals. Dealers should understand their clients' ownership and control structure. Ownership and control are not always synonymous. Trustees can control a trust without being beneficiaries. Where a corporation has voting and non-voting shares, ownership may be separate from control. Accordingly, sub-clause 3204(1)(iii) of the IIROC Rules refers to beneficial ownership or control "of the voting rights attached to the outstanding voting securities of a corporation". When establishing the identity of individuals who exercise control over the affairs of a partnership or trust, Dealers should identify those individuals who have the power to influence the trusts' or partnerships' affairs, regardless of the structure of the partnership or the trust.

4.7.2 Direct or indirect control

IIROC Rule 3200 requires Dealers to establish the identity¹⁵ of individuals who exercise "direct or indirect" control over 25% or more of a corporation. If a corporation is owned or controlled by other entities, the Dealer must identify those individuals who ultimately have beneficial ownership or control over its clients. Where a client has multiple owners, the Dealer should establish the ownership or control of each individual involved.

For example, if an individual owns 50% of the voting shares of a corporation that owns 25% of the voting shares the client, this individual owns directly 12.5% of the client. This individual's ownership falls below our 25% threshold, so the Dealer would not need to identify them. However, if the individual owned 100% of the voting shares of a corporation that owns 25% of the voting shares of the client, the Dealer must identify the individual as they indirectly owns 25%. We included a chart in **Appendix I** that shows the calculation of percentage indirect ownership in a multi-level ownership structure.

PCMLTF Regulations require Dealers to obtain the name and address of anyone owning, directly or indirectly, 25% or more of a corporation or other entity. By complying with IIROC Rule 3200, Dealers will comply with the PCMLTF Regulations.

¹³ See Appendix H for more details.

¹⁴ See IIROC Rule section 3206 and section 4.7.3 below for details.

¹⁵ See IIROC Rule section 3206 and section 4.7.3 below for details.



However, if a client is considered high risk, as a best practice, Dealers may consider whether to identify individuals who own or control less than 25%. For example, if a Dealer suspects that a client has an ownership structure designed to dilute or obscure the account's true beneficial owners, as a best practice, it may consider identifying individuals who own or control less than 25% of the company.

Dealers must record the measures taken and the information obtained in determining beneficial ownership. Dealers must maintain these records for all non-individual clients, regardless of their structure.

4.7.3 Establishing identity

IIROC Rule 3200 requires Dealers to establish the identity of:

- individual beneficial owners of 25% of corporations,
- individuals who exercise direct or indirect control or direction of 25% of corporations, and
- individuals who exercise control over partnerships and trusts.

This rule does not specify any method of establishing these individuals' identity. We require Dealers use "such methods that allow the Dealer to form a reasonable belief that it knows the identity of the individual and by taking reasonable measures to confirm the accuracy of the information obtained."¹⁶ The PCMLTF Regulations require Dealers "take reasonable measures to confirm the accuracy of the information obtained"¹⁷. FINTRAC's [Beneficial ownership requirements](#) guidance goes into detail on how Dealers should confirm this information.

Although the IIROC Rules do not specify a method, Dealers are required to comply with the PCMLTF Regulations as outlined in the following FINTRAC guidance:

- [Beneficial ownership requirements, and](#)
- [Ongoing monitoring requirements](#).

If a Dealer complies with the requirements outlined in this FINTRAC guidance, we would consider this a reasonable method of establishing the individual's identity.

4.7.4 Identity verification timing

IIROC Rule 3200 requires Dealers to establish the identity of beneficial owners and individuals who exercise control over corporations, partnerships and trusts "as soon as it is practicable, but not more than 30 days after opening the account." While 30 days is the maximum amount of time, Dealers should begin their efforts at as soon as possible. IIROC Rule 3200 is consistent with the PCMLTF Regulations, which require that the existence of the corporation or another entity be verified within 30 days of account opening.

¹⁶ See IIROC Rules, section 3206

¹⁷ See [s.11.1\(2\)](#) of the PCMLTF Regulations



Under section [11.1 of the PCMLTF Regulations](#), a Dealers can open an account for a corporation or another entity without obtaining and confirming details about its beneficial owners, beneficiaries and other controlling individuals, provided the Dealer meets certain conditions, including ascertaining the identity of the entity's most senior manager and treating that entity's activities as high risk.

However, under section 3206 of the IROC Rules, if a Dealer cannot establish the beneficial owners' and the controlling individuals' identity within 30 days, it must limit trading in the account.

If a Dealer cannot obtain and verify the necessary client information, it should review the situation to determine if any suspicious transaction reporting is required.

4.7.5 Exceptions to client identification requirements

Section 3207 of the IROC Rules contain exceptions for certain entities from our client identification requirements. Such entities include:

- Canadian financial institutions and their affiliates,
- Canadian securities registrants,
- Authorized foreign banks or Schedule III banks,
- Canadian pension funds, and
- Canadian public bodies or corporations (or their affiliates) with minimum net assets of \$75 million:
 - whose shares are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the Income Tax Act, and
 - who operate in a country that is a member of the Financial Action Task Force.

[Section 62\(2\)](#) of the PCMLTF Regulations contain similar exceptions, with some key distinctions. For instance, while the PCMLTF Regulations have exceptions for accounts where a Canadian financial institution or Canadian securities registrant provides instructions, our rules do not provide exceptions for these account types. However, Dealers must still comply with IROC KYC requirements. We expect Dealers will establish the identity of every client who owns a registered plan account in accordance with IROC Rule 3200.

4.7.5.1 Prohibition on shell banks

Sections 3205 of the IROC Rules prohibit Dealers from opening or maintaining accounts for any shell bank. Sub-section 3205(1) defines a shell bank as a bank that does not have any physical presence in any country.

The exceptions discussed in section 4.7.5 of this guidance do not exempt affiliates of Canadian financial institutions from this prohibition on shell banks.

4.7.6 Politically Exposed Persons and Heads of International Organizations

IROC Rules do not include any specific requirements on politically exposed persons or heads of international organizations. IROC Rule 3200 requires Dealers to use due diligence to learn and remain



informed of the essential facts relative to each client. We consider information collected under the PCMLTFA on a client's status as a politically exposed person or head of an international organization to be essential facts.

For more information on the PCMLTFA's politically exposed persons and heads of international organization requirements, consult FINTRAC's guideline "[Politically exposed persons and heads of international organizations – securities dealers](#)".

5. Key risk indicators for Dealers

Dealers can identify potential risk indicators based on specific client behaviour. In this section, we outline key risk indicators for Dealers. If a client exhibits any of the following behaviours or if the Dealer is concerned these behaviours could be occurring, it should investigate further.

Even if the Dealer decides not to open an account or conduct a transaction, it should consider whether it has reasonable grounds for filing a suspicious transaction report. Section 6 deals with suspicious transactions.

For more information on key money laundering and terrorist financing risk indicators, consult FINTRAC's guidance on "[Money Laundering and Terrorist Financing Indicators – Securities Dealers](#)".

5.1 Client due diligence risks

5.1.1 Clients with complex ownership structures

Some non-individual clients (such as trusts or corporations) can have complex ownership structures that obscure the true beneficial owners of the account. IIROC's client identity requirements in Part A of Rule 3200 are intended to "pierce the corporate veil" and identify the account's true beneficial owner. If the Dealer is finding it challenging to fulfill these requirements, it may be an indication of a complex ownership structure.

These clients can use off-book transactions, offshore accounts and nominees to further obscure true beneficial ownership. Clients may use accounts in one country as a "pass through" for accounts in other countries. This can indicate tax evasion, which is a predicate offence to money laundering.

If individuals want to use an entity to obscure the source of their funds or hide beneficial ownership, they may structure that entity's ownership to avoid our beneficial ownership requirements. For instance, an individual may hold 24.9% of an entity to avoid being caught above our 25% threshold. As a best practice in such cases, Dealers should consider identifying such beneficial owners.

While Part A of Rule 3200 requires Dealers to collect information on beneficial owners of 25% or more of a corporation, when faced with a client who is higher risk, as a best practice, a Dealer should consider identifying beneficial owners of less than 25%.



5.1.2 Using accounts for undeclared purposes

While Dealers are required to record the intended use of each client's account, it can be challenging to monitor whether the client is using its account for undeclared purposes. We expect the recorded intended use to be consistent with:

- client's KYC information, including its investment objectives and time horizon, and
- transactions in the client's account(s), including the types of securities purchased.

If not, the Dealer should conduct further investigation.

5.2 Trading risks

5.2.1 Over-the-Counter (OTC) securities

Companies with OTC securities are not required to provide much financial information. There is little demand for low cost or risky OTC securities, which are attractive to individuals, who can use them to move funds.

5.2.2 Stock manipulation

Some forms of stock manipulation occur when a client, acting alone or with an Approved Person, artificially inflates or deflates the price of securities to make a profit. This is an example of the criminal activity taking place within the market, which could be a predicate offence to money laundering. This risk may appear in conjunction with the OTC securities risk described in section 5.2.1.

5.2.3 Low-priced securities

While low-priced securities may indicate an under-valued issuer, they could also be associated with fraudulent or potentially fraudulent companies. This risk may appear in conjunction with the OTC security risk in section 5.2.1, but may also be present with publically traded issuers on regulated markets. If a client frequently trades in low-priced securities this could indicate suspicious activity, especially if:

- the client immediately liquidates or transfers the proceeds, or
- the client does not provide a reasonable rationale for the trade.

Trading in low-priced securities could be used by individuals to obscure the trace of the funds.

5.2.4 Inactive issuers and shell companies

If an issuer does not have an active business or an active investor base, this could be an indication of a shell company. Shell companies are often used by individuals to launder money. Other indicators of a shell company include:

- no brick and mortar locations or locations which are shared with other companies or law firms,
- frequent changes to name, business plan or structure, or
- issuer information is hard to obtain or is fraudulent or misleading.



Trading in shell companies or inactive issues could indicate potential money laundering or fraud.

5.3 Non-trading risks

5.3.1 Cash deposits or withdrawals

Almost all client accounts at Dealers are funded by either account transfers from other firms or direct deposits from Canadian banks or credit unions. Funds are usually removed from accounts in similar ways. As such, most transactions are conducted with other Canadian financial institutions subject to the same AML rules. If a client requests a cash deposit or withdrawal directly from the Dealer, this could be an indicator of potential money laundering or terrorist financing as the client would remove funds from the regulated Canadian financial system.

5.3.2 Physical certificates deposits

The vast majority of securities are now traded electronically and physical certificates are rare. When physical certificates are deposited into a brokerage account, there is little information confirming the source of funds or how the client obtained them. As a result, there is a greater risk that they could be used by criminals to obscure the source of their money.

5.3.3 Early redemption of securities

Certain GICs and mutual funds can incur fees when sold early or prior to maturity. If a client is selling securities early and incurring a fee without a plausible explanation, this could indicate money laundering. Criminals may invest in these products to hide the source of their wealth and then sell them, making their money “clean”.

5.3.4 Requesting proceeds in the form of negotiable instruments

Proceeds of the sale of securities are typically held within a client’s account(s), usually to be reinvested or transferred to its bank account. Individuals might instead ask for the proceeds using bank drafts or certified cheques to disguise the true source and ownership of the funds.

5.3.5 Transfer of funds between accounts

Individuals may transfer money frequently between accounts, theirs or their family members’, to layer transactions and distance their money from its criminal origin. Dealers should be suspicious of accounts used solely as conduits to transfer funds without legitimate securities transactions.

Likewise, Dealers should also be wary of frequent changes of ownership between accounts of related or connected individuals and cross-border money movements.

6. Suspicious transactions

FINTRAC has issued the following guidelines on suspicious transactions:

- [Money laundering and terrorist financing indicators - Securities dealers](#),
- [What is a suspicious transaction report](#), and
- [Reporting suspicious transactions to FINTRAC](#).



6.1 Account Supervision requirements

IIROC Rule 3900 requires Dealers supervise all account activities to ensure compliance with IIROC requirements, securities laws and other applicable laws, including the PCMLTF Regulations and the PCMLTFA.¹⁸

Dealers' policies and procedures should provide for, amongst other things:

- identification of clients presenting a high AML risk to the Dealer,
- identification of clients presenting a high risk of conducting improper activities in the securities markets, and
- screening of trading activity to detect issues for further enquiry or investigation.

Dealers should consider "high risk" to include a high risk of conducting fraudulent securities activities, which are predicate money laundering offences and/or could be indications of money laundering and terrorism funding.

[IIROC's Universal Market Integrity Rules \(UMIR\)](#) Rule 7.1 also includes trade supervision requirements that apply to Dealers who are also Participants¹⁹. For the purposes of UMIR 7.1, a supervision system must consist of both policies and procedures aimed at preventing violations from occurring and compliance procedures aimed at detecting whether violations have occurred.

IIROC Rule 3900 also requires Dealers' account supervision programs to detect the following (among other items):

- unsuitable trading,
- excessive trade activities,
- trading in restricted securities,
- excessive trade transfers and trade cancellations indicating possible unauthorized trading,
- inappropriate or high risk trading strategies,
- excessive or improper crosses of securities between clients,
- manipulative and deceptive activities, and
- insider trading.

The PCMLTFA requires that Dealers report attempted and completed suspicious transactions. The PCMLTFA and PCMLTF Regulations also require Dealers to conduct ongoing monitoring of their business relationships with clients. Dealers can use their account supervision program to meet the AML rules' transaction and activity monitoring requirements.

For example, Dealers may detect suspicious transactions through account supervision. Insider trading and manipulative and deceptive trading activities are considered predicate money laundering offences under the [Criminal Code \(RSC 1985, c. C-46\)](#). If a Dealer detects these types of activities through its

¹⁸ See IIROC Rule 3900, clause 3904(2)(ii).

¹⁹ See section 1.1 of UMIR for a definition of "Participant".



supervision program, it should consider reporting these activities to FINTRAC as a suspicious transaction. It is very difficult to separate a transaction that is part of a market-based criminal offense from a transaction designed to launder the proceeds of crime.

Dealers can find information on common suspicious transactions in the securities industry in the FINTRAC report, [Money Laundering Trends and Typologies in the Canadian Securities Sector](#).

6.2 Account Supervision programs and ongoing monitoring

A Dealer Member's account supervision program can range from the manual monitoring of significant transactions or activities to the use of automated supervision systems²⁰. Once a Dealer Member determines the appropriate method to supervise account activity effectively, it should adopt appropriate related procedures.

The frequency and nature of the monitoring should be commensurate with the risk level of the business relationship. More frequent monitoring will be required for high-risk business relationships. A Dealer's policies and procedures should document at minimum:

- the actual monitoring processes,
- the required frequency, and
- the rationale to support the monitoring processes.

Dealers should use the Business Relationship Record to determine whether transactions or activities are consistent with the client's information, including that client's risk assessment. The ongoing monitoring program can detect suspicious transactions and indicate when a Dealer should reassess the client's risk level.

Although Dealers frequently use risk-based supervision and monitoring procedures and focus on higher risk products, services and clients, they are still required to monitor all clients and business relationships. For example, while Dealers may decide to monitor high risk clients more frequently than low risk clients, they must still monitor low risk clients. "Low risk" is not "no risk" and Dealers should pay attention to all types of suspicious activities.

Dealers should compare individual transactions to other account activities and the client's profile to determine whether they are suspicious. Dealers should examine transactions seeming to lack a reasonable economic basis or recognizable strategy based on the particular client.

Dealers should provide examples of potentially suspicious activity to all appropriate personnel and incorporate these into their anti-money laundering policies, procedures and training materials. Dealers should advise their employees that they must escalate and report any suspicious activity to FINTRAC.

²⁰ The use of an automated supervision system may require IIROC approval or discussion. Please contact your Business Conduct Compliance Manager.



6.3 Enhanced measures for high risk business relationships

Dealers can also implement additional enhanced measures for high-risk clients beyond frequently updating client identification information and more frequent monitoring of client activity. FINTRAC's [Compliance program requirements](#) guidance includes a list of potential enhanced measures Dealers can take.

6.4 Other Compliance and Supervision systems and procedures

Dealers may find reviewing gatekeeper reports on market manipulation or insider trading filed under [UMIR Rule 10.16](#) to be helpful sources when determining which transactions should be reported to FINTRAC as suspicious.

Dealers should also review improper activities by employees or agents such as internal theft, fraud or conspiracy to manipulate a market to determine whether to report them to FINTRAC as a suspicious transaction.

7. U.N. suppression of terrorism reports and similar requirements

Dealers are required to check client names against the lists of designated individuals and organizations under Canadian economic sanctions and report monthly on the results. Further information can be found on IIROC's website under "[Sanctions Reporting System](#)".

Dealers must conduct monthly reporting through the [IIROC Services](#) portal.

From time to time, the federal government passes other regulations that amend the reporting requirements.

Access to the password-protected reporting system is limited to authorized persons at each firm. Dealers should have policies and procedures to ensure that client name checks are done and reports are filed on time. In addition, there must be a back-up for the person responsible for the reporting and a succession plan and training in case that person is not available.

8. Applicable Rules

IIROC Rules this Guidance Note relates to:

- Rule 1400,
- Rule 3200, Part A and
- Rule 3900.

9. Previous Guidance Notes

This Guidance replaces:

- the IIROC [Anti-Money Laundering Compliance Guidance](#), and
- [MR0294](#) – Amendments to Regulation 1300.1 Identification of Beneficial Owners of Non-Individual Accounts.



10. Appendices

- Appendix A** - Client Due Diligence and Large Cash Transaction Requirements
- Appendix B** - Background
- Appendix C** - Penalties for Violations of PCMLTFA
- Appendix D** - Classification of Violations for Determining Administrative Penalties
- Appendix E** - Members of FATF
- Appendix F** - Stock Exchanges Recognized Under Section 262(1) of the *Income Tax Act* in FATF Member Countries
- Appendix G** - Reference Material
- Appendix H** - Client Identification and Verification Requirements Comparison Chart
- Appendix I** - Beneficial Ownership Diagram



Appendix A: Client Due Diligence and Large Cash Transaction Requirements

Information on the PCTFMLA, the PCTFML Regulations' client due diligence and large cash transaction requirements can be found here:

- (i) FINTRAC Guidance:
 - [Beneficial ownership requirements](#)
 - [Business relationship requirements](#)
 - [Guidance on the Risk-Based Approach to Combatting Money Laundering and Terrorist Financing](#)
 - [Methods to identify individuals and confirm the existence of entities](#)
 - [Ongoing monitoring requirements](#)
 - [Politically exposed persons and heads of international organizations – securities dealers](#)
 - [Risk-based approach workbook for securities dealers](#)
 - [Suspicious transaction reporting guidance](#)
 - [Third party determination requirements](#)
 - [When to identify individuals and confirm the existence of entities – Securities dealers](#)
- (ii) [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Regulations](#)
- (iii) [Proceed of Crime \(Money Laundering\) and Terrorist Financing Act](#)



Appendix B: More Information on Money Laundering Legislation

1. Money Laundering Under the Criminal Code

The [Criminal Code \(RSC 1985, c. C-46\)](#) establishes offences on the possession of and dealings in the proceeds of crime, money laundering and the financing of terrorism.

1.1 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 it was obtained by or derived from the commission of an indictable offence.

[Section 462.31](#) of the *Criminal Code* addresses money laundering. It is 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.

[Section 462.3\(1\)](#) of the *Criminal Code* defines a designated offence, often called a predicate offence, as any indictable offence under any Act of Parliament other than offences established by regulations.

Designated offences of particular interest to Dealers 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 client due diligence and reporting requirements under various regulations described below.
- Bribery and corruption because of the provisions regarding secret commissions and the PCMLTFA requirements regarding politically exposed foreign persons described in this guidance.

Dealers should also be aware of the wide variety of designated offences, including:

- Possession of or trafficking in scheduled substances under the [Controlled Drugs and Substances Act](#).
- Deceptive telemarketing contrary to the [Competition Act](#).
- Smuggling and evasion of duties contrary to the [Customs Act](#).
- Unlawful manufacture, packaging, stamping or sale of tobacco products contrary to the [Excise Act](#).

1.2 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, the maximum penalty is two years' imprisonment. The maximum penalty for a money laundering conviction is 10 years' imprisonment.

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

1.3 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.

2. PCMLTFA Requirements Applicable to Dealers

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

The requirements for financial institutions to implement anti-money laundering mechanisms are based on *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (RSC 2000, c. 17) (**PCMLTFA**).

2.2 Regulations

Most of the specific AML/ATF requirements are contained in regulations under PCMLTFA. The five regulations applicable to Dealers are:

- The [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Regulations](#) which govern cash transaction reporting, client due diligence, compliance and recordkeeping.
- The [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Suspicious Transaction Reporting Regulations](#) which govern the reporting of completed and attempted suspicious transactions.
- The [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Administrative Penalties Regulations](#) which set out FINTRAC's ability to impose administrative penalties.
- The [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Registration Regulations](#) which set out the registration requirements for entities also conducting money services activities
- The [Cross-border Currency and Monetary Instruments Reporting Regulations](#) which establish reporting requirements for cross-border movements of funds and monetary instruments.

2.3 Offences and Penalties under PCMLTFA

Violations of the PCMLTFA can result in up to a \$2 million fine and 5 years' imprisonment for the most serious offences.



2.4 Administrative Penalties

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.

FINTRAC can reduce the penalty by half if the violator enters into a compliance agreement with FINTRAC.

[Part 4.1 of PCMLTFA](#) contains more details on the procedures for imposition of administrative penalties.



Appendix C: Penalties for Violations of PCMLTFA

This information is available on FINTRAC's [Penalties for non-compliance website](#).



Appendix D: Classification of Violations for Determining Administrative Penalties

This information is available on FINTRAC's [Administrative monetary penalties website](#).



Appendix E: Members of FATF (Financial Action Task Force)

This information is available on FATF's [FATF Members and Observers](#) website.



Appendix F: Stock Exchanges Recognized Under Section 262(1) of the *Income Tax Act* in FATF Member Countries

This information is available on the Department of Finance's [Designated Stock Exchanges website](#).



Appendix G: Reference Material

Financial Action Task Force Recommendations

FATF Recommendations	http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf
----------------------	---

Additional Guidance

FATF Money Laundering FAQ	http://www.fatf-gafi.org/faq/moneylaundering/
FATF: Risk-based Approach Guidance for the Securities Sector	http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-securities-sector.html
FATF: Canada's measures to combat money laundering and terrorist financing	http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-canada-2016.html
FINTRAC Information for Securities Dealers containing a high level outline of	http://www.fintrac-canafe.gc.ca/re-ed/sec-eng.asp
Minister of Finance – Ministerial Directives	FINTRAC website – Ministerial directives and transaction restrictions



Appendix H: Client Identification and Verification Requirements Comparison Chart

Requirement	AML Rules	IIROC Rules
Beneficial owners and beneficiaries (information firms must collect on the client)	Information on the ownership, control and structure of the entity And Corporations : <ul style="list-style-type: none"> Names of all directors Names & addresses of those who own or control 25% or more of the shares of a corporation Entities other than corporations: <ul style="list-style-type: none"> names and addresses of those who own or control 25% or more of the entity Trusts : <ul style="list-style-type: none"> the names and addresses of all trustees and all known beneficiaries and settlors of the trust 	Identity of: <ul style="list-style-type: none"> beneficial owners of more than 25% of a corporation individuals who exercise control over affairs of a partnership or trust Names & addresses of: <ul style="list-style-type: none"> all directors of a corporation all trustees, known beneficiaries and settlors of a trust
Establishing identity	<ul style="list-style-type: none"> confirm information 	<ul style="list-style-type: none"> establish information (as per s.3206 in Appendix C)
Timing (how long firms have to verify/establish/	Entities - 30 days Individuals – before the first transaction other than the initial	<ul style="list-style-type: none"> 30 days

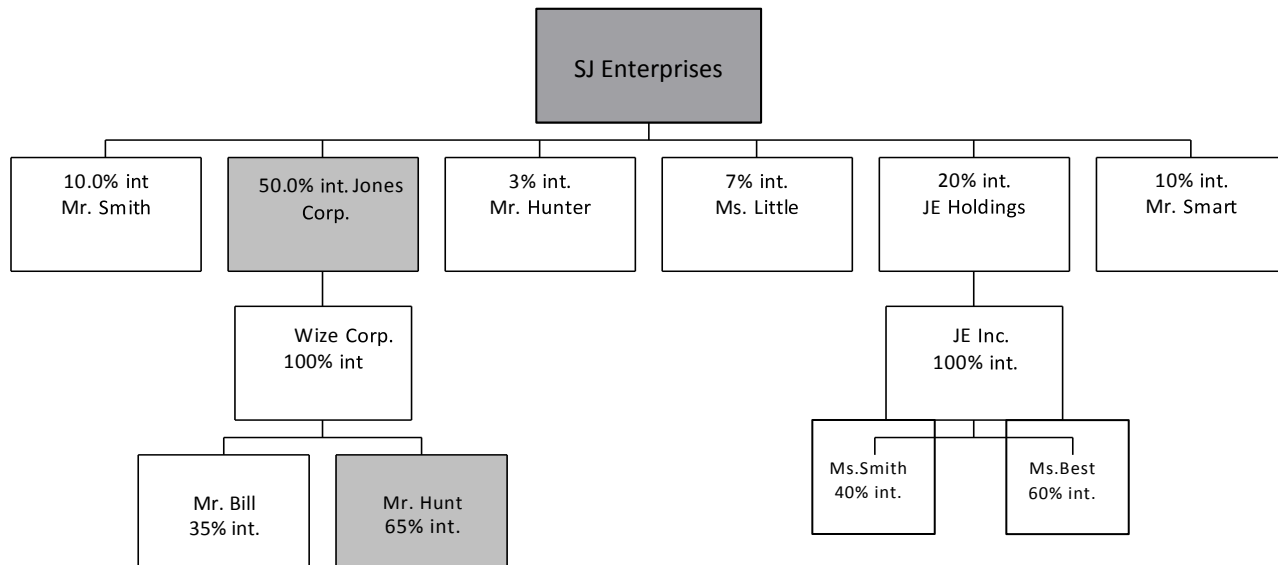


Requirement	AML Rules	IIROC Rules
confirm the information)	deposit	
Exceptions	<ul style="list-style-type: none"> • financial entity or affiliate that carries banking, life insurances or securities activities (bank, credit union, caisse populaire, trust and loan companies) • registered plans • regulated pension fund • securities dealer • investment fund • life insurance company • public body or large publicly-traded corporation 	<ul style="list-style-type: none"> • Canadian registered firm • Canadian investment fund • Canadian financial institution • Schedule III bank • public body or large publicly-traded corporation <p>(Note: the Rule Amendments clarify that foreign financial entities are not exempt.)</p>



Appendix I: Beneficial Ownership Diagram

This diagram shows the calculation of percentage indirect ownership in a multi-level ownership structure:



<i>Individual</i>	<i>Ownership Calculation (of SJ Enterprises)</i>	<i>Is Beneficial Ownership Information Required?</i>
Mr. Bill	$0.35 \times 1.00 \times 0.50 = 0.175 = 17.5\%$	No*
Mr. Hunt	$0.65 \times 1.00 \times 0.50 = 0.325 = 32.5\%$	Yes
Ms. Smith	$0.40 \times 1.00 \times 0.20 = 0.080 = 8.00\%$	No*
Ms. Best	$0.60 \times 1.00 \times 0.20 = 0.120 = 12.0\%$	No*
Mr. Smith	10.0%	No*
Mr. Hunter	3%	No*
Ms. Little	7.0%	No*
Mr. Smart	10%	No*

*Beneficial ownership information may be required if the client is high risk or if there are any red flags.