



ANTI MONEY LAUNDERING (AML) AND ANTI-TERRORIST FINANCING (ATF) POLICY

AKAL Mortgages Inc. o/a AKAL Mortgages

238 Britannia Rd E

Mississauga, ON L4Z 1S6

AKALmortgages.com | Tel: (416) 621-1300

Lic. #s: ON 10845 | SK 514018 | NS 3000827 | Independently owned and operated

Adoption of the Policy

AKAL Mortgages Inc. o/a AKAL Mortgages is an entity that is authorized under provincial legislations (Ontario, British Columbia, Alberta, Saskatchewan and Nova Scotia) to act as a mortgage brokerage (the “Brokerage”)¹. The Brokerage employs individuals who are authorized under provincial legislations to act as mortgage brokers (for simplicity, the “Broker”). On behalf of the Brokerage, the Broker help borrowers find suitable mortgages by collecting borrower data and sharing it with various potential lenders. The selected lender then works with the borrower to fund and complete the mortgage. Once the mortgage is completed, the lender pays a commission for the benefit of the Brokerage and Broker.

Since the Brokerage and Brokers are authorized under provincial legislation(s) to act as intermediaries between a lender and a borrower with respect to loans secured by mortgages on real property or hypothecs on immovables, the Brokerage and Brokers fall within the definition of “mortgage broker” for the purposes of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the PC Act). Mortgage brokers are subject to the requirements of the PC Act because they are engaged in a business or profession for the purposes of paragraph 5(i) of the PC Act. As individuals and entities in Canada, the Brokerage and Brokers are also subject to Canadian sanctions legislation.

Purpose of AML/ATF Policy

The Brokerage has established these anti-money laundering, anti-terrorist financing and sanctions compliance policy and procedures (“AML Policy or Policy”) to comply with the requirements of the PC Act and Canadian sanctions legislation and to set out the measures that the Brokerage has implemented in respect of its operations to prevent the misuse of its products and services to launder money, finance terrorist activities, or contravene Canadian economic sanctions (“AML Program”).

Money laundering, terrorist financing, and sanctions violations are significant problems facing governments and payment service providers around the world. To combat these problems, Canada has enacted laws that require financial institutions, money services

businesses and other financial intermediaries to detect and help prevent money laundering, the financing of terrorism, and sanctions violations.

Money laundering, terrorist financing, and sanctions violations also present risks to the Brokerage. The reputation of the Brokerage can be significantly damaged as a result of any association with money laundering, terrorist financing, or sanctions violations. In addition, the Brokerage and Broker can face penalties for failing to comply with applicable Canadian requirements. Potential penalties include criminal prosecution, costly and public civil penalties, and regulatory enforcement actions.

BROKERAGE INFORMATION:

Mortgage Brokerage (MB):	AKAL Mortgages Inc. o/a AKAL Mortgages
Licence No.:	ON 10845 SK 514018 NS 3000827
Primary Place of Business:	238 Britannia Rd E Mississauga, ON L4Z 1S6
Main Telephone:	(416) 621-1300
Compliance Officers (COs)	ON — Rashmeet Kaur BC AB NS — Kuljit Singh SK — Mohinder Pal Singh
Office Telephone:	(416) 621-1300
Email:	info@AKALmortgages.com

Table of Contents

1. INTRODUCTION	6
2. THE REQUIRED OVERALL COMPLIANCE PROGRAM FOR BROKERAGES	8
3. APPOINTMENT OF A COMPLIANCE OFFICER	9
4. RISK ASSESSMENT	11
5. TRAINING PROGRAM	12
6. TWO-YEAR EFFECTIVENESS REVIEW	13
7. REPORT TRANSACTIONS	15
8. RECORD KEEPING REQUIREMENTS	23
9. KNOW YOUR CLIENT (“KYC”)	25
10. MINISTERIAL DIRECTIVES AND TRANSACTION RESTRICTION	49
1. APPENDIX 1: DEFINITIONS	51
2. APPENDIX 2: DETAILED PROCEDURES FOR RISK ASSESSMENT DEVELOPMENT	81
3. APPENDIX 3: TRAINING	93
4. APPENDIX 4: STRS	94
5. APPENDIX 5: LISTED PERSON OR ENTITY PROPERTY REPORTS (LPEPRS)	96
6. APPENDIX 6: LCTR	99
7. APPENDIX 7: LVCTR	103
8. APPENDIX 8: DUAL-PROCESS METHOD	107

1. Introduction

The content of this policy addresses the Canadian financial crime compliance regulatory obligations applicable to Mortgage Brokers under the following legislation and regulations:

- Proceeds of Crime (Money Laundering) and Terrorist Financing Act (“PCMLTFA”) Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (“PCMLTFR”)
- Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (“PCMLTFSTR”)

Source: [Mortgage administrators, brokers and lenders \(canada.ca\)](https://www.canada.ca/en/mortgage-administrators-brokers-lenders/canada.ca)

This Policy addresses the regulatory requirements applicable to the mortgage sector effective October 11, 2024, together with subsequent amendments and FINTRAC guidance. This policy should be read in conjunction with local AML and ATF Procedures (“Procedures”). The following entities/persons in the mortgage sector are subject to the above Act and its respective Regulations:

- Mortgage Administrators*
- Mortgage Brokers*
- Mortgage Lenders*

1.1 What is Money Laundering?

Money laundering is the process used to disguise the source of money or assets derived from criminal activity. There are three recognized stages in the money laundering process:

1. **Placement** involves placing the proceeds of crime in the financial system.
2. **Layering** involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the trail and the source and ownership of funds. This stage may involve transactions such as the buying and selling of stocks, commodities or property.
3. **Integration** involves placing the laundered proceeds back into the economy to create the perception of legitimacy.

The money laundering process is continuous, with new 'dirty' money constantly being introduced into the financial system.

1.2 What is Terrorist Activity Financing?

Terrorist activity financing is the use of funds, property or other services to encourage, plan, assist or engage in acts of terrorism, where the primary motivation is not financial gain.

Two main differences distinguish terrorist activity financing from money laundering:

Funds can be from legitimate sources, not just criminal acts; and

Money is the means, not the end—the goal is to use funds to facilitate or implement terrorist activities.

1.3 FINTRAC Universal Enrolment – Pending Coming into Force

Legislative amendments establish a universal enrolment requirement for businesses subject to the PCMLTFA that are not otherwise required to register. This requirement will come into force in line with regulations to be developed and published in the Canada Gazette, Part II. The Compliance Officer will monitor the regulations and FINTRAC guidance and will ensure that the Brokerage applies for and maintains enrolment within the prescribed timelines once the requirement comes into force.

1.4 FINTRAC's role and threats to security of Canada

FINTRAC's role is to provide CSIS with financial intelligence to assist that agency in fulfilling its mandate of investigating threats to the security of Canada. Threats to the security of Canada are defined in the Canadian Security Intelligence Service Act as:

1. espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage;
2. foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive, or involve a threat to any person;
3. activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state; and,
4. activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of the constitutionally established system of government in Canada, but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).
5. and intelligence agencies.

FINTRAC occupies an important position in the constellation of organizations involved in Canada's fight against money laundering and terrorism. Each of these organizations has a particular relationship with FINTRAC. Due to the nature of its mandate, the

Centre's work is situated at the beginning of a process that starts with the reports to FINTRAC by financial institutions and intermediaries. With the assistance of specialized automated tools, skilled staff analyze the reported transactions and information from other sources to extract financial intelligence that would be relevant to the investigation or prosecution of money laundering offences, terrorist activity financing offences, and threats to the security of Canada.

Money laundering and terrorist financing cases can be extremely complex, often involving many players implicated in transnational and covert illicit activity. The investigations are often time and resource intensive. For this reason, the time between FINTRAC's initial disclosure and the conclusion of an investigation can be quite lengthy.

FINTRAC's core product is case-specific financial intelligence. FINTRAC is also well situated to provide strategic intelligence about trends and typologies of money laundering and terrorist financing. Because money laundering and terrorist financing are almost always transnational in character, and because an important part of FINTRAC's role is to exchange information with like bodies in other countries, it is also well placed to provide a strategic overview from an international perspective.

2. The Required Overall Compliance Program for Brokerages

The implementation of the compliance program is key to the success of meeting the local regulatory requirements and addressing financial crime risk in general. There are key elements to a compliance program which include:

1. The **appointment of a Compliance Officer**, who is responsible for the implementation of the compliance program, and the role which is further outlines in the "Appointment of a Compliance Officer" section
2. The development and application of **written compliance policies and procedures** that are kept up to date and in the case of senior management are approved by a Senior Officer
3. A **risk assessment** of the business to assess and document the risk of a money laundering offence or a terrorist activity financing offence occurring in the course of business activities
4. An Ongoing Compliance **Training Program**
5. A Two-Year Effectiveness **Review Plan**

6. Know Your Client (**KYC**) Program
7. Business Relationship and Ongoing **Monitoring** Requirements
8. **Record** Keeping Requirements
9. **Reporting** Requirements
10. Ministerial Directives

The proceeding sections of the policy outline in detail the requirements for each compliance program element that will need to be addressed in the policy and the corresponding procedures to meet the requirements of the PCMLTFA and its respective Regulations for Mortgage Brokers.

3. Appointment of a Compliance Officer

The Compliance Officers (COs) identified in the Brokerage Information section of this Policy have been appointed for their respective jurisdictions and are responsible for the implementation and oversight of AKAL Mortgages Inc.'s AML/ATF compliance program within those jurisdictions.

If the MB is a small business or sole employee-run, the owner or senior manager is delegated as the CO. If the MB is a large business, the CO must be appointed and have unfettered direct access to senior management and the board of directors

The CO is not involved in receiving, transferring, or paying funds. The CO has independent oversight and communicates directly with parties who make decisions about the business, including senior management or the board of directors

The CO is responsible for implementing the compliance program, and simply appointing one does not mean that the compliance program requirements have been met. For the CO to succeed, the CO must:

- Have the necessary authority and access to resources in order to implement and make any desired changes to the compliance program
- Have knowledge of the business's function and structure.
- Have knowledge of the business sectors' money laundering and terrorist financing risks and vulnerabilities.
- Have knowledge of the different money laundering trends and typologies and
- Understand the MB requirements under the PCMLTFA and its associated Regulations.

A CO may delegate specific duties to other employees but is ultimately responsible for implementing that component in relation to the compliance program. Although the review of the activity may be centralized as part of the operations department, the responsibility for the implementation and ultimate quality of the program lies with the CO.

The CO or delegate is responsible for creating or developing the AML/ATF Policy and Procedures. The CO is responsible for keeping the policy up to date in relation to new legislative changes and typologies and reviewing the policy annually. The CO is also responsible for getting the policy approved annually by a Senior Officer if the MB is not a sole employee business.

This AML/ATF Policy, including any material amendments, will be reviewed and approved at least annually by Kuljit Singh, Co-Founder and Chief Executive Officer and Director of AKAL Mortgages Inc., acting in his capacity as Senior Officer.

The responsibilities of the Compliance Officer include the following:

1. ensuring the AML Policy is developed and implemented effectively, including monitoring compliance by the Brokerage's brokers and other employees with their obligations under the AML Program;
2. reviewing this Policy and related controls as needed (and at least annually) and proposing updates following recent amendments to legislation and regulatory expectations, and changes to the Brokerage's business or assessed AML or sanctions risks;
3. implementing, documenting, and maintaining an ongoing AML and sanctions compliance training program for the Brokerage's brokers, officers and other employees;
4. ensuring that an effectiveness review of the Brokerage's AML Program is conducted at least every two years by a qualified external or internal auditor;
5. the content of this policy addresses the current Canadian financial crime compliance
6. obligations applicable to mortgage administrators, mortgage brokers and mortgage lenders,
7. including amendments and FINTRAC guidance in force as of September 19, 2026;
8. ensuring that records required under this Policy are maintained so that they are readily available to FINTRAC on request;
9. developing and implementing procedures for reporting to FINTRAC, the Royal Canadian Mounted Police (RCMP), and Canadian Security Intelligence Service (CSIS), as required by law;

10. monitoring for any directives that may be issued by the Minister of Finance under Part 1.1 of the PC Act and ensuring that this Policy is updated, as necessary, to address the requirements of such directives; and
11. following developments and best practices in AML/ATF and sanctions measures.

On an ongoing basis, the Compliance Officer and compliance team members routinely review notices from FINTRAC and other relevant government sources regarding new or amended legislation, regulations, guidance and business practices, and will evaluate the applicability to the operations of the Brokerage and will take appropriate steps to update this Policy and any applicable procedures accordingly.

The Compliance Officer will be responsible for advising the Brokerage's business units about any material changes in the Brokerage's obligations under Canadian AML and sanctions legislation.

4. Risk Assessment

This policy reflects requirements applicable to the mortgage sector from October 11, 2024, together with subsequent amendments and FINTRAC guidance through September 19, 2026. This policy should be read in conjunction with local AML and ATF Procedures ("Procedures"). The following entities/persons in the mortgage sector are subject to the Act and its respective Regulations:

1. the Brokerage's borrowers and business relationships with borrowers;
2. the Brokerage's products, services and delivery channels;
3. the geographic location of the Brokerage's activities; and
4. the risk of relying on the Brokers to deliver the Brokerage's products and services.

The Compliance Officer will be responsible for preparing and updating the Brokerage's written AML/ATF risk assessment and ensuring that the risk assessment and reassessments are documented and follow the framework set out in FINTRAC's Risk assessment guidance, as it is amended from time to time. The Brokerage's risk assessment will also be informed by the Government of Canada's Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada. ²

Based on a risk assessment, the Brokerage will assign a risk rating to every borrower (low, medium, and high). All borrowers rated as high risk will be subject to the enhanced risk-mitigation requirements outlined in this Policy.

The Brokerage has established a tolerance level in respect of its exposure to money-laundering and terrorist-financing risks. Business activities and relationships that expose

² <https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/rba/rba-eng>

the Brokerage to risks above the established risk tolerance level will not be engaged in or entered into.

Please see Appendix 2: Risk Assessments for more details on the development of Risk Assessments by the Compliance officer.

5. Training Program

As part of the compliance program, an ongoing training program must be implemented and maintained and is the responsibility of the CO. The target audience of the training program includes employees, brokers, mandataries or other authorized persons (collectively, employees). This training program will ensure that employees are adequately trained to understand the requirements of Canadian AML and sanctions legislation, as well as the regulatory expectations of FINTRAC. The training is designed to encourage a culture of compliance at the Brokerage. This training is required yearly for all affected employees. Employees new to the Brokerage or to a relevant position will be required to complete the training as part of their onboarding process before they are dealing with borrowers.

The training program at a minimum will be tailored to the roles and responsibilities of the employees, and must include:

- MBs are required to meet all the requirements under the PCMLTFA and its associated Regulations.
- Definition of money laundering and terrorist financing and how they are reflected in the mortgage sector
- How MB are vulnerable to money laundering and terrorist financing activity (indicators and examples)
- The compliance policy and procedures that have been developed to meet the requirements under the PCMLTFA and its Regulations for preventing and detecting money laundering and terrorist financing, including reporting, record keeping and knowing your client's requirements
- Roles and responsibilities in detecting and deterring money laundering and terrorist financing activities when dealing with potentially suspicious activities/transactions for MBs, brokers, employees.

The training is tailored to each employee, broker, and mandatory's responsibilities. The training program is commensurate with the brokerage's size, type, nature and complexity. As part of the training program, a written training plan will be documented outlining the implementation of the ongoing training program including how the training will be delivered. The plan includes information about:

- Training recipients
- Training topics and materials
- Training methods for delivery and
- Training frequency

5.1 Training recipients

The training plan must outline who will receive training, including those who:

- Have contact with clients
- Are involved in client transactions
- Handle cash, funds or virtual currency; and
- Are responsible for implementing or overseeing the compliance program (CO, senior management, KYC/CDD team, internal auditors, information technology staff)

Please see Appendix 3 for more information about training topics and materials.

6. Two-Year Effectiveness Review

The two-year effectiveness review is conducted every two years at a minimum and is used to test the effectiveness of elements of the compliance program. Those elements include:

- Policies and procedures
- Risk assessment
- Ongoing training program and plan

The Compliance Officer is responsible for conducting the effectiveness review and it must commence 24 months after the previous one. The last review must be completed before the next one begins.

The effectiveness review aims to identify gaps and weaknesses within the compliance program that may impact whether money laundering and terrorist financing are prevented or detected. The review should determine if:

- The business activities reflect what is outlined in the compliance program documentation and if those activities meet the requirements under the PCMLTFA and its associated Regulations.

- The risk assessment effectively identifies and mitigates money laundering and terrorist financing risks related to clients, products, services, delivery channels, new developments or technology, and geographic locations.

An internal or external auditor documents the results. The review must be conducted by someone knowledgeable of the MB requirements under the PCMLTFA and its associated Regulations. As part of best practices, it is not performed by someone directly involved in the compliance program activities to ensure impartiality.

A documented plan for the two-year effectiveness review must be instituted and documented. The plan describes the scope of the review and includes a focus on all the compliance program elements. The depth of the review is impacted by the complexity of the business, transaction volume, findings from previous reviews and current money laundering and terrorist financing risk. The plan also includes the rationale supporting the focus area, the time period to be reviewed and the anticipated evaluation methods and sample sizes. The following are examples of what is required to be included in the review, please include all that apply for your Brokerage:

- Interviews with those handling transactions to evaluate their knowledge of the policies and procedures and related record-keeping, client identification and reporting requirements;
- Review a sample of records to assess whether client identification policies and procedures are being followed;
- Review agreements with brokers or mandataries, as applicable, as well as a review of a sample of the information that brokers or mandataries referred to verify the identity of persons, to assess whether client identification policies and procedures are being followed;
- Review transactions to assess whether suspicious transactions were reported to FINTRAC;
- Review large cash transactions to assess whether they were reported to FINTRAC with accurate information and within the prescribed timelines;
- Review virtual currency transactions to assess whether reportable transfers were reported to FINTRAC with accurate information and within the prescribed timelines (applicable to RE sectors that have LVCTR obligations);
- Review a sample of client records to see whether the risk assessment was applied in accordance with the risk assessment process;
- Review a sample of client records to see whether the frequency of ongoing monitoring is adequate and carried out in accordance with the client's risk level assessment;
- Review a sample of high-risk client records to confirm that enhanced mitigation measures were taken;

- Review a sample of the records to confirm that proper record-keeping procedures are being followed;
- Review the risk assessment to confirm that it reflects current operations and
- Review the policies and procedures to ensure that they are up to date, reflect current legislative requirements, and reflect current business practices.

The review also includes the following pieces of information:

- The date the review was conducted, the period covered by the review, and the person or entity who performed the review;
- The results of the tests performed; and
- The conclusions, including deficiencies, recommendations, and action plan (if any)

The Effectiveness Review must be reported in writing to a senior officer no later than 30 days after the completion of the review:

- The findings of the review (e.g. deficiencies, recommendations, action plans)
- Updates made to policies and procedures during the reporting period (the period covered by the review) that were not made because of the review and
- The status of the implementation of the updates to the policies and procedures

If the MB is a sole-employee business, an effectiveness review still needs to be conducted and include the above elements. Since the MB is a sole employee, there is no need to issue the report to senior management. It should be noted that there are no exceptions to completing a two-year effectiveness review.

7. Report Transactions

Under the PCMLTFA and its respective Regulations, MBs are required to report on any of these types of events:

- Suspicious Transaction Report *[this includes not only transactions but also activities]*
- Listed Person or Entity Property Report (LPEPR)
- Large Cash Transactions Reports [AKAL Mortgages does not accept cash from clients.]
- Large Virtual Currency Transaction Report [AKAL Mortgages does not accept virtual currency from clients.]
- Sanctions Evasion

The following sections of this policy outline the reporting requirements for each of the above report types applicable to Mortgage Brokers.

7.1 Suspicious Transaction Report

A Suspicious Transaction Report (“STR”) is a type of report that must be submitted to FINTRAC when a financial transaction occurs or is attempted in the course of activities, and there are [reasonable grounds to suspect](#) that the transaction is related to the commission or the attempted commission of a money laundering or terrorist activity financing offence.

The MB is prohibited from tipping off a client. This is where the client has been informed of the content of the STR or that a report will be made or filed with FINTRAC. This applies whether an investigation has begun or not. Since it is crucial that the client is not tipped off about an STR being filed, the MB should only request information that is normally requested during a transaction if it is believed that the client would be tipped off due to the request.

MBs and their respective employees must report suspicious transactions. Where the person is an employee of the MB and the MB is actively reporting suspicious transactions, the employee is not required to report to FINTRAC. In the rare instance where an employee believes that their employer has not submitted a STR in accordance with the PCMLTFA and its associated Regulations, the employee will use the [paper form](#).

A service provider can also submit a STR on behalf of the MB. Where an MB has engaged a service provider to submit a form on their behalf, the MB is ultimately responsible for meeting the requirements under the PCMLTFA and its Regulations. The legal responsibility cannot be delegated. Where a service provider is obtained to submit reports on behalf of the entity, all arrangements are entered via a written agreement. For further information on service provider arrangements, please click on the [link](#) to the FINTRAC website.

All financial transactions attempted or completed where there are reasonable grounds to suspect that they are related to the commission or attempted commission of money laundering or terrorist financing must be reported to FINTRAC.

Reasonable grounds to suspect are the required threshold to submit an STR to FINTRAC. They are a step above simple suspicion, meaning that there is a possibility that a money laundering or terrorist activity financing offence has occurred. It is not required to verify the facts, context, or money laundering or terrorist activity financing indicators that led to the suspicion, nor is it required to prove that a money laundering or terrorist activity financing offence has occurred to reach this threshold.

The suspicion must be reasonable and, therefore, not biased or prejudiced. To reach the threshold, the following must be considered:

- The facts;
- The context;
- The money laundering or terrorist financing indicators, see [link](#);
- The sanctions evasion characteristics, see the [link](#);

If, after considering the above information, it could be concluded that there are reasonable grounds to suspect that the particular financial transaction is related to the commission of money laundering or terrorist financing, report the transaction. By reaching the threshold for reasonable grounds, one should be able to clearly demonstrate and articulate the suspicion of money laundering or terrorist activity financing. For further information on what constitutes reasonable grounds, please click on the [link](#).

When in receipt of a production order from law enforcement related to a predicate offence, assess the facts, context, and money laundering or terrorist activity financing indicators to determine whether there are reasonable grounds to suspect that a particular transaction is related to the commission of a money laundering or terrorist activity financing offence.

7.1.1 When To Submit a STR

An STR must be submitted as soon as practicable after completing measures that establish reasonable grounds to suspect that the transactions or attempted transaction is related to the commission of a money laundering or terrorist financing offence. As soon as practicable, it means that the following measures have been completed, which have led to the determination that the reasonable grounds to suspect threshold have been met and that the submission of the STR must be prioritized. It should be noted that no monetary threshold is associated with reporting a suspicious transaction.

Measures to help establish reasonable grounds include:

- Screening for and identifying suspicious transactions;
- Assessing the facts and context surrounding the suspicious transaction;
- Linking money laundering or terrorist activity financing indicators to the assessment of the facts and context;
- Explaining the grounds of suspicion in an STR needs to articulate how the facts, context, **money laundering and terrorist activity financing indicators** allowed one to reach the grounds for suspicion.

A [fact](#), for the purpose of completing a STR, is defined as an event, action, occurrence, or element that exists or is known to have happened or existed. It cannot be an opinion. An example would be the date of the transaction. That would be a fact.

[Context](#), for the purpose of completing a STR, is defined as information that clarifies the circumstances or explains a situation or transaction. This type of information is essential to differentiate between what may be suspicious and what may be reasonable in each scenario.

One may observe or understand the context of a transaction through:

- A general awareness of the events occurring in a person or entity's business environment or community;
- Knowledge of the typical financial activities found within the MB's business;
- Regular [know your client](#) activities (for example, verifying the identity of persons and entities, their occupation or business, how they generate their source of wealth and typical or expected transactional behaviours);
- The information obtained through the application of the [risk assessment](#);
- Illustrative client details (for example, the financial background, behaviour and actions of the Client).

A transaction may not appear suspicious in and of itself. However, a review of additional contextual elements surrounding the transaction may create suspicion. Conversely, the context of a particular transaction, which may have seemed unusual or suspicious from the onset, could lead to a reassessment of a client's current and past transactions and a conclusion that they are reasonable.

The suspicion of money laundering or terrorist activity financing will likely materialize from the assessment of multiple elements (transactions, facts, context, and any other related information that may or may not be an indicator of money laundering or terrorist activity financing. When these elements are viewed together, they create a picture that will either support or negate the suspicion of the commission of a money laundering or terrorist activity financing offence.

7.1.2 Money Laundering and Terrorist Activity Financing Indicators or Sanctions Evasions Characteristics

Money laundering and terrorist activity financing indicators, as well as sanctions evasion characteristics, are potential red flags that can initiate suspicion and indicate that something may be unusual without a reasonable explanation. Red flags typically stem from one or more facts, behaviours, patterns or other contextual factors that identify irregularities related to a client's transactions. These often present inconsistencies with

what is expected or considered normal based on the facts and context of what is known about the client and their transactional activities.

Criminal organizations often use concealment methods to try to avoid the detection of money laundering or terrorist activity financing. Indicators of money laundering and terrorist activity financing can bring to light suspicious transactional activity. Still, the holistic assessment of facts, context, and money laundering and terrorist activity financing indicators will enable the determination of whether reasonable grounds have been reached. Explaining how reasonable grounds for suspicion are met is extremely important for FINTRAC's development and disclosure of financial intelligence.

Money laundering indicators can be found [here](#). FINTRAC also publishes strategic intelligence documents that focus on the identification of money laundering or terrorist activity financing-related methods, techniques, and vulnerabilities, which can be found [here](#). For further information on the characteristics of financial transactions involved in suspected sanctions evasion, see [here](#).

Please see Appendix 4 for more information about STRs.

7.2 Reporting Listed Person or Entity Property

Listed Person or Entity Property Report (“LPEPR”) requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations apply to all reporting entities, including mortgage brokers. An LPEPR must be submitted to FINTRAC immediately when the Brokerage is required to make a disclosure concerning property under section 83.1 of the Criminal Code, an order or regulation made under the United Nations Act, an order or regulation made under the Special Economic Measures Act, or subsection 7(2) of the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law).

7.2.1 What is Considered a Property?

Property is anything owned or controlled by a [person](#) or [entity](#), whether tangible or intangible. It includes real and personal property, deeds, and instruments that give a title or right to property or to receive money or goods. It also consists of any property that has been converted, exchanged or acquired from any conversion or exchange.

The following are examples of property for the purpose of an LPEPR:

- [Cash](#);
- Monetary instruments (for example, cheques, bank drafts or money orders);

- Casino products and tokens;
- [Virtual currency](#) (VC);
- Accounts (for example, personal or business accounts, Registered Retirement Savings Plans (RRSP), Tax-Free Savings Accounts (TFSA);
- [Prepaid payment products](#) and [prepaid payment product accounts](#);
- Securities (for example, stocks, bonds or mutual funds);
- [Jewellery](#), [precious metals](#) or [precious stones](#);
- Real estate, including an instrument that gives title or right to a property (for example, a deed); and
- Insurance policies.

Physical goods (for example, equipment, vehicles or artwork). An LPEPR must be submitted to FINTRAC immediately when the applicable disclosure obligation is triggered. All reporting must be done in good faith.

7.3 Criminal Code

Under [subsection 83.1\(1\)](#) of the Criminal Code, **every person in Canada** and **every Canadian outside Canada** must disclose without delay to the Commissioner of the Royal Canadian Mounted Police (RCMP) or to the Director of the Canadian Security Intelligence Service (CSIS) the existence of property in their possession or control that they know is owned or controlled by or on behalf of a **terrorist group**. In addition, any information about the transaction or proposed transaction concerning that property must be disclosed to the RCMP or CSIS. According to subsection 83.01, a terrorist group is defined as:

- An entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity;
- A **listed entity** or
- An association of such entities.

A listed entity is one that appears on a list established under section 83.05 of the Criminal Code. This list is a way of identifying whether groups or individuals are associated with a terrorist group; see the [Public Safety Canada list](#). An entity could include a person, group, trust partnership or fund, or an unincorporated association or organization. Through normal transactions, other sources of information may help determine that a client is associated with or part of a terrorist group. These instances include:

- Publicly available information or media articles stating that the client has carried out or facilitated terrorist activity or

- Official, publicly available lists relating to terrorist activity (for example, the Office of Foreign Assets Control (OFAC) and European Union (EU) lists).

7.3.1 Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST)

Under subsection 8(1) of the RIUNRST, every person in Canada, every Canadian outside Canada, and certain prescribed entities must disclose without delay to the Commissioner of the RCMP or the Director of CSIS the existence of property in their possession or control that they have reason to believe is owned, held or controlled by or on behalf of a listed person. In addition, this information must be disclosed to the RCMP or CSIS about a transaction or proposed transaction regarding such property.

According to section 1 and subsection 2(1) of the RIUNRST, a listed person is an individual or entity that is listed in the Schedule of the RIUNRST because there are reasonable grounds to believe that the individual or entity:

- has carried out, attempted to carry out, participated in or facilitated the carrying out of a terrorist activity;
- is controlled directly or indirectly by any such individual or entity or
- Criminal Code, United Nations Act, SEMA and Magnitsky Act Requirements

The Brokerage must consider applicable disclosure obligations under section 83.1 of the Criminal Code and applicable orders or regulations made under the United Nations Act, the Special Economic Measures Act (SEMA), and the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law). The listed person or entity framework expands the former terrorist-property reporting regime to include terrorist and sanctioned property.

7.4 A listed person or entity may include a terrorist group as defined in subsection 83.01(1) of the Criminal Code; a person or entity subject to an order or regulation under the United Nations Act or SEMA; a foreign state subject to an applicable order or regulation; or a person subject to an order or regulation under section 4 of the Sergei Magnitsky Law.

- Where the applicable legislation requires disclosure of property to the RCMP or CSIS or another prescribed authority, the Brokerage must make that disclosure without delay and must also submit the required LPEPR to FINTRAC immediately.
- The Compliance Officer must ensure that current Canadian sanctions and terrorist listings are incorporated into the Brokerage's screening and escalation procedures.

See the Procedures for the current screening sources, escalation steps, disclosure channels and reporting instructions.

LPEPRs differ from other reports submitted to FINTRAC because a transaction or attempted transaction does not need to occur. The existence of property owned or controlled by or on behalf of a terrorist group, listed person or listed entity may itself trigger the disclosure and reporting obligations.

- Where the applicable disclosure threshold is met, the Brokerage must make the required disclosure to the appropriate authority and submit an LPEPR to FINTRAC immediately.
- Submit an LPEPR to FINTRAC immediately in accordance with FINTRAC's current reporting method.

LPEPRs support the detection of terrorist activity financing and sanctions evasion networks and form part of Canada's AML/ATF and sanctions-evasion regime.

Please see Appendix 5 for more information about LPEPRs.

Please see Appendix 6 for Large Cash Transaction report, if your Brokerage accepts cash or deals in cash transactions, and include it in your policies and procedures.

Please see Appendix 7 for Large Virtual Currency Transaction report, if your brokerage accepts virtual currency, or deals in virtual currency, and include it in your policies and procedures.

7.5 Sanctions Evasion Reporting

All transactions must be reported to FINTRAC when completed or attempted where there are reasonable grounds to suspect the transaction is related to the commission or attempted commission of a sanction evasion offence. Sanctions evasion offence means an offence arising from the contravention of a restriction or prohibition established by an order or a regulation made under the United Nations Act, the Special Economic Measures Act or the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law). Where there are reasonable grounds to suspect sanctions evasion by someone acting on behalf of a sanctioned person, these transactions must be submitted to FINTRAC as STRs. For further guidance on reporting suspicious transactions, see the section on **STR** within the policy.

If a transaction is suspected of being related to both a money laundering or terrorist financing offence and a sanctions evasion offence, submit one report containing details and all required information for each of the suspected offences.

For information on the characteristics of financial transactions related to suspected sanctions evasion, see the [link](#) to the Special Bulletin on Financial Activity Associated

with Suspected Sanction Evasion on the FINTRAC website. Also, consult FINTRAC's [joint financial intelligence advisory on Russian end-users' illegal procurement of dual-use goods](#). This advisory supports recognizing financial transactions and other related activity suspected of being associated with laundering the proceeds linked to the purchase and sale of dual-use goods for illegal export from Canada.

Apply the following ministerial directives with respect to:

- [Russia](#)
- [Islamic Republic of Iran](#)
- [Democratic People's Republic of Korea](#)

For information on Ministerial Directives, including the **associated obligations**, consult [Ministerial directives and transaction restrictions](#).

7.6 Listed Person or Entity Property Reporting

Where it has been determined that the Brokerage possesses or controls property that meets an applicable terrorist or sanctions disclosure threshold, a Listed Person or Entity Property Report must be submitted immediately as outlined in the section on Reporting Listed Person or Entity Property and the Procedures.

8. Record Keeping requirements

Record Keeping Requirements

A record of the following must be kept for 5 years.

- Copies of every report sent to FINTRAC:
 - STRs
 - Listed Person or Entity Property Reports
 - Large Cash Transaction Reports
 - Large Virtual Currency Transaction Reports
- Large cash transaction records when the MB receive \$10,000 CAD or more in cash in a single transaction
- Large virtual currency transaction records when the MB receives virtual currency in an amount equivalent to \$10,000 CAD or more in a single transaction
- [Receipt of funds](#) records when the MB receives any amount in connection with a mortgage on real property or a hypothec on immovables

- [Information records](#) in the following circumstances:
 - In the case of a mortgage broker, when they arrange a mortgage loan
- Mortgage loan records, which includes:
 - The financial capacity of the client
 - The terms of the loan
 - The nature of the client's principal business or their occupation, and
 - The name and address of their business or place of work if the client is a person
- Copies of the part of official corporate records containing any provision relating to the power to bind the corporation if the receipt of funds record or information record is for a corporation
- Beneficial ownership records
- Politically exposed persons records
- Client identification records
- Records related to any business relationship and ongoing monitoring
- Third party determination records

Where there is currently no FINTRAC guideline available to MB's on their specific record keeping obligations, consult the [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Regulations](#) for more information.

It should be noted that information for occupation and type of business must be specific. As an example, the occupation as a Manager is vague. More detailed information is acceptable such as Hotel Reservation Manager. Vague business information is not acceptable. For example, the business is identified as "Retail", is vague and unacceptable. A more acceptable answer is the business is a chain of 20 locations selling bath and fitting fixtures, with an ecommerce presence. The more information provided in the occupation and type of business the better to assist with ongoing monitoring and the detection of suspicious transactions.

More detailed information on the process of record keeping can be found in the Procedures.

Exceptions to Record Keeping

Where there are record keeping requirements regarding certain information, and that information is available in another record, that information does not need to be recorded again.

Records are not required to be kept of large cash transaction, a large virtual currency transaction or a receipt of funds records if the amount received is from:

- a [financial entity](#)
- a [public body](#)
- a person acting on behalf of a client that is a financial entity or a public body

9. Know Your Client (“KYC”)

There are several instances where KYC activity needs to be undertaken, and specification verification methods must be applied. Those activities include:

9.1 Transactions and Business Records

1. The MB must verify the identity of any person or entity for the following transactions or when a business record needs to be kept.
 - Suspicious transactions
 - Large cash transactions
 - Large virtual currency transactions
 - Receipt of funds records
 - Information Records
 - Mortgage Loan Records

9.2 Business Relationships

2. For mortgage administrators, mortgage brokers and mortgage lenders, a business relationship is established the first time the reporting entity is required to verify the identity of a client under the Regulations. The client’s identity must be verified in accordance with the applicable timing, method and record-keeping requirements.

9.3 Third-Party Determination

3. Measures must be taken to determine whether a third party is involved when:
 - Reporting a large cash transaction or keeping a large cash transaction record
 - Reporting a large virtual currency transaction or keeping a large virtual currency transaction record

- Keeping an information record

9.4 Politically Exposed Persons (PEP)

4. When entering into a business relationship or receiving an amount of \$100,000 or more in cash or virtual currency, reasonable measures must be taken to determine whether the following people are being dealt with:
 - A politically exposed domestic person;
 - A politically exposed foreign person;
 - A head of an international organization;
 - A family member of a person who is closely associated with one of those persons
 - A close associate of one of those persons (for the cash or virtual currency transaction or if the MB detects a fact related to a business relationship);
 - A close associate of a politically exposed foreign person (for business relationships).

For the above KYC Sections 1-4, the next section of this policy outlines explicitly the verification methods and other specific policy requirements that MBs must undertake.

9.4.1 Verification Methods

Specific methods are permitted when verifying the identity of a person or entity. This ensures that the information in an identification document or from other informational sources matches the information the person or entity provides.

There are five permissible methods allowed for verifying a person's identity. They include:

- Government-issued photo identification method;
- Credit file method;
- Dual-process method;
- Affiliate or member method; and
- Reliance method.

9.4.1.1 Government Issued photo identification method

This method involves verifying the person's identity by referring to a government-issued photo identification document. The document must:

- Be authentic, valid, and current;

- Be issued by a federal, provincial or territorial government (or by a foreign government if it is equivalent to a Canadian document);
- Indicate the person's name;
- Include a photo of the person;
- Include a unique identifying number and
- Match the name and appearance of the person being identified.

Photo identification documents issued by municipal governments, Canadian or foreign, are not acceptable. See the following [link](#) for acceptable forms of identification.

Determination of whether a government-issued photo identification document is **authentic, valid, and current** can be done by viewing it **in person** and by looking at the characteristics of the original physical document and its security features (or markers, as applicable) **in the presence of the person being identified**. This allows the verifier of the information to be satisfied that the identification document is authentic, as issued by the competent authority (federal, provincial, or territorial government), is valid (unaltered, not counterfeit), and current (not expired).

9.4.1.2 Government-issued photo identification method - Person not physically present

Where a person being verified is not present, technology must be used to determine the document's authenticity. As an example:

- Ask a person to scan their government-issued photo identification document using the camera on their mobile phone or electronic device and
- Use technology to compare the features of the government-issued photo identification document against known characteristics (for example, size, texture, character spacing, raised lettering, format, design), security features (for example, holograms, barcodes, magnetic strips, watermarks, embedded electronic chips) or markers (for example, logos, symbols) to be satisfied that it is an authentic document as issued by the competent authority (federal, provincial, or territorial government).

When a person is not physically present, MBs are still required to determine whether the authenticated government-issued photo identification document is **valid** and **current** and that the name and photo are those of the person providing the document. As an example:

- Participate in a live video chat session with the person and compare the name and the features of the live video image to the name and photo on the authentic government-issued photo identification document or

- Ask the person to take a "selfie" photo using the camera on their mobile phone or electronic device and use an application to apply facial recognition technology to compare the features of that "selfie" to the photo on the authentic government-issued photo identification document.

For further information on the processes followed to determine whether a government-issued photo identification document is authentic, whether the client is present or not, and how to confirm that the identification document is valid and current, it is documented in the procedure. In addition, the procedures describe the steps taken to confirm that the name and photograph are those of the person.

9.4.1.3 Record-keeping requirements for the government-issued photo identification method

When using the government-issued photo identification method, a record must be kept of:

- The person's full name;
- The date on which the MB verified the person's identity;
- The type of document used (for example, driver's licence, passport, etc.);
- The unique identifying number of the document used;
- The jurisdiction (province or state) and country of issue of the document; and
- The document's expiry date, if available (if this information appears on the document or card, the MB must record it).

9.4.2 Credit File Method

A person's identity may be verified using the credit file method. The credit file method must:

- Contain information that is valid and current;
- Be from a Canadian credit bureau (credit files from foreign credit bureaus are not acceptable);
- Have been in existence for at least three years;
- Contain information that is derived from more than one source (i.e. more than one tradeline); and
- Match the name, address and date of birth of the identified person.

The credit assessment does not need to be requested or included in verifying the person's identity. To execute the credit file method, the search must be conducted at the time when the person is being identified. A credit file cannot be provided by the person or be of one that was previously obtained. It is acceptable to use an automated system to match the person's information with the information in the person's credit file. A third-party vendor may be used when obtaining valid and current information from the person's credit file. If any of the information provided by the person (name, address or date of birth) does not match the information in the credit file, this verification method cannot be used. Another vendor can provide another credit file, or another verification method can be used.

Information in the credit file may contain a variation in the name or a discrepancy in the address provided. A determination must be made as to whether the information in the credit file matches the information provided by the person. As an example:

- If there is a slight typo in the address or name, it is possible to determine that the information still matches what the person provided;
- If there is a discrepancy in their date of birth, it is more likely that it is determined that the information does not match;
- Suppose there are multiple addresses in the credit file. In that case, it is possible that the address provided by the person is not the primary address but does appear in the credit file as a secondary address. If this is the case, the MB can still meet the requirements to ensure that the information matches what the person provided.

9.4.2.1 Record-keeping requirements for credit file method

When using the credit file method, it is important to keep a record of the following:

- The person's name;
- The date the credit file was consulted or searched;
- The name of the Canadian credit bureau or third-party vendor as the source holding the credit file and
- The person's credit file number.

Review the procedures to understand:

- The process of verifying the person's identity;
- How to ensure information is valid and current;
- Alternate steps are to be taken if the information is not valid or current.

9.4.3 Dual-Process Method

Another verification method is the dual process method, which consists of doing any two of the following:

Method A

- Referring to information from a reliable source that includes the person's **name and address** and confirming that the name and address are those of the person;

Method B

- Referring to information from a reliable source that includes the person's **name and date of birth** and confirming that the name and date of birth are those of the person or

Method C

- Referring to information that includes the person's **name and confirms that they have a deposit account, a credit card, or other loan account with a financial entity**, and verifying that information.

The information **must** be valid and current **and** come from two different reliable sources. This information could be found in **statements, letters, certificates, forms or other sources that can be provided through an original version or** another version of the information's original format, such as a fax, a photocopy, a scan, or an electronic image. For example, a fax, photocopy, scan, or electronic image of a government-issued photo identification document can be relied upon as one of the two pieces of information required to verify a person's identity.

The same source cannot be used for two categories that are being used to verify a person's identity. As an example, if in the verification process, reliance is made on a bank statement from Bank ABC, which contains the person's name and address, reliance cannot be made on another bank statement for a deposit account from Bank ABC, which contains the person's name. Bank ABC would be the same source for both categories.

The possible combinations for this method can vary based on what the client has. The combinations include:

Method A and Method B

Referring to information from one reliable source that includes the person's **name** and **address** and confirming that this matches the information provided by the person, **and** referring to information from a different reliable source that consists of the person's **name** and **date of birth** and confirming that this matches the information provided by the person.

OR

Method A and Method C

Referring to information from one reliable source that includes the person's **name** and **address** and confirming that this matches the information provided by the person and referring to information from a different reliable source that consists of the person's **name** and a **financial account** (specifically, a deposit account, a prepaid payment product account, a credit card account or a loan account) and confirming this information.

OR

Method B and Method C

Referring to information from one reliable source that includes the person's **name** and **date of birth** and confirming that this matches the information provided by the person and referring to information from a different reliable source that includes the person's **name** and a **financial account** (specifically, a deposit account, a prepaid payment product account, a credit card account or a loan account) and confirming this information.

Note: If the information does not match the information provided by the person, it cannot be relied on. For example, it is **not acceptable** to rely on information if the account number or number that is associated with the information is truncated or redacted. Occasionally, information from a source may contain a variation on the client's name or a typo in the client's address. In these instances, a determination must be made as to whether the information matches the information provided by the person. If there is a slight typo in the address or a misspelled name, it may be determined that the information still matches what the person provided. However, in the case of an incorrect

date of birth, it is more likely that it will be determined that the information does not match. In this case, reliance cannot be made on the information from this source for identification purposes. Information from a different source under the dual-process method or using a different method (for example, the government-issued photo identification method or the credit file method) must be made to verify the person's identity.

Please see Appendix 8 for more information on the dual-process method.

9.4.4 Reliance Method

The identity of a person may be verified by relying on measures previously taken by:

- Another RE (person or entity that is referred to in section 5 of the PCMLTFA)

To rely on measures previously taken by **another RE** to verify the identity of a person, the MB must:

- As soon as feasible, obtain from the **other RE** the information that was confirmed as being that of the person, and be satisfied that:
 - The information is valid and current, and
 - The **other RE** verified the person's identity using the government-issued photo identification method, the credit file method or the dual-process method, or if the **other RE** verified the person's identity prior to June 1, 2021, that they did so in accordance with the PCMLTFR, by using the methods that were in place at the time; **and**
- Have a written agreement or arrangement with the **other RE** that, upon request, requires them to provide, as soon as feasible, all the information that they referred to in order to verify the person's identity.

9.4.4.1 Record-keeping requirements for the reliance method

MB, when relying on another RE to verify the identity of a person, must keep a record of

- The person's name;
- The written agreement or arrangement with the other RE to verify a person's identity and
- The information that the other RE referred to verifies the identity of the person.

The procedures describe the process that must be followed when using the reliance method to verify a person's identity and the approach taken to ensure the information is

valid and current.

9.4.5 A Broker or Mandatary to Verify the Identity of a Person on the MB's Behalf

The MB can verify a person's identity by using a broker or mandatary to carry out the verification on the MB's behalf, in accordance with the government-issued photo identification method, the credit file method, or the dual-process method.

Measure can be relied upon to verify a person's identity that was previously taken by a broker or mandatary if they were:

- Acting in their own capacity at the time, whether they were required to use the methods by the PCMLTFR or
- Acting as a broker or mandatary under a written agreement or arrangement that was entered into with another RE to verify a person's identity using either the government-issued photo identification method, the credit file method or the dual-process method, or if the measures were taken prior to June 1, 2021, using the methods in accordance with the PCMLTFR that were in place at the time.

9.4.5.1 Using a Broker or Mandatary

When using a broker or mandatary to conduct verification measures, a few elements need to be in place:

- A written agreement in place before they are used
- Obtain as soon as feasible, all the information that the broker or mandatary referred to verify the person's identity and the information that the broker or mandatary confirmed as being that of the person; and
- Be satisfied that:
 - The information that the broker or mandatary confirmed as being that of the person is valid and current, and
 - The person's identity was verified using the government-issued photo identification method, the credit file method or the dual-process method, or, if the person's identity was verified prior to June 1, 2021, using the methods in accordance with the PCMLTFR in place at the time.

9.4.5.2 Record-keeping requirements when using a broker or a mandatary

When verifying the identity of a person by using a broker or mandatary, a record must be kept of:

- The person's name;

- The written agreement or arrangement with the broker or mandatary for verifying a person's identity; and
- All the information the broker or mandatary referred to in order to verify the identity of the person and the information that the broker or mandatary confirmed as being that of the person (this includes, as applicable, information that is required to be kept in the record for the method used).

Note: MBs are responsible for meeting client identification requirements under the PCMLTFA and associated Regulations, even when using a broker or mandatary to verify a person's identity on the MB's behalf or when relying on the measures previously taken by a broker or mandatary to verify a person's identity.

9.4.5.3 Verifying a person's identity if they have been previously verified

A person's identity does not need to be identified for subsequent transactions if their identity was verified using one of the above methods.

Note: In the context of a business merger or acquisition, the client does not need to be re-identified if the acquired clients were verified in accordance with the methods outlined in the PCMLTRF at the time. Where new clients are acquired, client information is updated in accordance with the risk assessment process. The "new" clients become the responsibility of the MB, which must ensure compliance with the PCMLTFA and its associate Regulations.

Although the PCMLTFR provides guidance regarding identifying a child, no one under 18 is allowed to establish a business relationship with the MB.

9.5 How to Verify the Identity of an Entity

There are three acceptable methods MBs can use to verify the identity of an entity:

- a) Confirmation of existing method
- b) Reliance method
- c) Simplified identification method

While an entity can be a corporation, a trust, a partnership, a fund, or an unincorporated association or organization, **corporations are subject to different requirements than other entities (as explained below).**

9.5.1 Confirmation of Existence Method

9.5.1.1 To verify the identity of a corporation refers to:

- A certificate of incorporation;
- A record that must be filed annually under provincial securities legislation or
- The most recent version of any other record that confirms the corporation's existence and contains its name and address and the names of its directors, such as a certificate of active corporate status, the corporation's published annual report signed by an audit firm, or a letter or notice of assessment for the corporation from a municipal, provincial, territorial or federal government.

You can choose one of the approaches; however, the record must be authentic, valid, and current. A corporation's name, address, and directors' names may be obtained from a publicly accessible database, such as a provincial or federal database like the [Corporations Canada database](#) or a corporation search and registration service through subscription.

When a corporation is a securities dealer, the names of its directors do not need to be confirmed when confirming its existence.

9.5.1.2 To verify the identity of an entity other than a corporation refers to:

- A partnership agreement;
- Articles of association; or
- The most recent version of any other record that confirms its existence and contains its name and address.

The record must be authentic, valid, and current.

9.5.1.3 Record-Keeping Requirements when Verifying the Identity of a Corporation or Other Entity (Confirmation of Existence Method)

MBs must keep records when they verify a corporation or an entity other than a corporation. Those records include:

- Keeping a copy of the paper record or an electronic version of that record
 - If the electronic version of the record is kept in a database accessible to the public, keep a record that includes the corporation or other entity's registration number, the type of record referred to and the source of the electronic version of the record.

Refer to the procedures that outline the steps MB must follow when using the confirmation of existence method to verify the identity of corporations and other entities and ensure that the information is authentic, valid, and current.

9.5.2 Reliance Method

The Reliance Method, in general, allows the verification of a corporation or an entity other than a corporation by:

- Another reporting entity (a person or entity that is referred to in section 5 of the PCMLTFA);

9.5.2.1 Measures Previously Taken by Another Reporting Entity

When relying on measures taken by another reporting entity to verify the identity of a corporation or an entity other than a corporation, the following must be met:

- As soon as feasible, obtain from the other RE the information that was used to confirm the identity of the corporation or other entity, as the case may be, and be satisfied that:
 - The information is valid and current, and
 - For a corporation, its identity was verified by the other RE by referring to a record as described in the confirmation of existence method above, or if the measures to verify the corporation's identity were performed prior to June 1, 2021, that the other RE confirmed the corporation's existence and ascertained its name, address, and the names of its directors in accordance with the methods in the PCMLTFR as they read at that time; and
 - For an entity other than a corporation, its identity was verified by the other RE by referring to a record as described in the confirmation of existence method above or if the measures to verify the entity's identity were performed prior to June 1, 2021, the other RE confirmed the entity's existence in accordance with the methods in the PCMLTFR as they read at that time; and
 - Have a written agreement or arrangement in place with the other RE that, upon request, requires them to provide the MB, as soon as feasible, with all the information that they referred to in order to verify the identity of the corporation or other entity, as the case may be.

The procedures outline the process to be followed when using the reliance method to verify the identity of a corporation and entities other than a corporation and how to ensure the information is valid and current.

9.5.3 Simplified Identification Method

The simplified identification method may be used to verify a corporation or entity's identity and meet the obligations under the PCMLTFA and its regulations.

As of the writing of this policy, it currently applies to those reporting entities that are in paragraphs 5(a) to (g) of the PCMLTFA, and currently, it is unclear whether the simplified identification method will apply to MB. However, the subsequent policy section will address the Simplified Identification Method as a potential method to undertake. However, it is the responsibility of the MB as of October 11, 2024, to confirm whether this method is applicable.

The simplified method requires that the risk related to the corporation or entity other than a corporation is risk-rated low for money laundering and terrorist financing offences and if:

- The corporation or other entity whose identity is being verified:
 - a. Is referred to in any of paragraphs 5(a) to (g) of the PCMLTFA;
 - b. Is a foreign corporation or entity that carries out activities that are similar to those of an entity referred to in any of paragraphs 5(a) to (g) of the PCMLTFA;
 - c. Administers a pension or investment fund that is regulated under the legislation of a foreign state and that a foreign government creates either or is subject to the supervision of a competent authority under the legislation of that foreign state;
 - d. Is one whose shares are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the Income Tax Act;
 - e. Is a subsidiary of a corporation or an entity that is referred to in paragraphs a. to d. in this section and is one whose financial statements are consolidated with the financial statements of that corporation or entity;
 - f. Is an institution or agency of, or in the case of a corporation, is owned by, the government of a foreign state; or
 - g. Is a public service body, as defined in subsection 123(1) of the Excise Tax Act; and
- The MB is satisfied that, within the applicable period for which the corporation or entity had to have their identity verified, the corporation or other entity exists and that every person who deals with you on behalf of the corporation or other entity is authorized to do so.

If, after subsequent consideration based on the risk assessment, the risk of money laundering or terrorist financing offences is no longer low, as soon as possible, verify the identity of the corporation or other entity type by referring to the appropriate records as

outlined in Confirmation of Existence Method.

9.5.3.1 Record-Keeping Requirements when Verifying the Identity of a Corporation or Other Entity (Simplified Identification Method)

MBs are required to keep records when they verify a corporation or an entity other than a corporation using the simplified identification method. Those records include:

- The grounds for considering there is a low risk of a money laundering offence or terrorist activity financing offence and
- The information obtained about the corporation or other entity, as the case may be, and about the persons that provided assurance that the corporation or other entity exists and that the persons the MB deals with are authorized to act on behalf of the corporation or the entity.

The procedures outline the process to be followed when using the simplified method to verify the identity of a corporation and entities other than a corporation and how to ensure the information is valid and current.

9.5.3.2 Restrictions on the Use of Personal Information

The use of personal information in Canadian commercial activities is protected by the Personal Information Protection and Electronic Documents Act (PIPEDA) or by similar provincial legislation. The MB must inform clients about the collection of their personal information. Clients do not need to be informed when their personal information is used in reports that are required to be submitted to FINTRAC.

See the link to see a high-level summary of the following on the FINTRAC website in the Annex section of the guidance:

- Methods to identify persons and associated record-keeping obligations;
- Who can identify the person;
- Methods to identify an entity and related record-keeping obligations;
- Examples of acceptable photo identification documents;
- Examples of reliable sources of information for the dual process method.

9.5.4 Business Relationships

What is a business relationship? For mortgage administrators, mortgage brokers and mortgage lenders, a business relationship is established the first time the MB is required under the Regulations to verify the identity of the client. This mortgage-sector rule applies

to the client-identification triggers described in this Policy, subject to applicable statutory and regulatory exceptions.

- The business relationship begins when the first applicable obligation to verify the client's identity arises.
- The Compliance Officer must ensure that the Procedures identify the transaction and record-keeping events that trigger identity verification, including suspicious transactions, large cash transactions, large virtual currency transactions, receipt-of-funds records, information records and mortgage-loan records.

Where an exception removes the underlying obligation to verify identity for a particular client, transaction or activity, the effect of that exception on formation of a business relationship must be assessed under the applicable Regulations and current FINTRAC guidance.

Where the underlying obligation to verify identity exists but the Regulations permit the MB not to re-verify or otherwise provide relief from repeating verification, the business relationship requirement must still be considered. The Procedures must document how these circumstances are handled.

- **Suspicious Transaction Reporting**

Reasonable measures must be taken when identifying a person or entity conducting or attempting to conduct a transaction. Despite whether the measures are unsuccessful or if doing the reasonable measures might have resulted in tipping off the person or entity that an STR might be filed, this transaction must factor into the business relationship requirement.

- **Re-verifying Identity**

Business relationship requirements must still factor in transactions or activities for which there is a requirement to verify identity but also allow for it not to happen. The regulations allow for re-verification not to occur if

- The client was previously identified using methods identified in the PCMLTFR;
- The associated records were kept, and
- There are no doubts about the information used

9.5.5 Business Relationship Records

A record must be kept of the following when entering into a business relationship. A record should be kept of:

- Purpose and intended nature of the business relationship
- Describe the business dealings with the client and
- Include information that would help anticipate the type of transactions and activities the client may conduct. This information could assist in identifying usual or suspicious transactions/activity while the MB conducts ongoing monitoring.

If this information is available in other accessible records and can be provided to FINTRAC, then an additional record is not required.

A business relationship ends when a period of at least five years has passed since the day of the last transaction that required the MB to verify the identity of the client.

9.5.6 Ongoing Monitoring

Ongoing monitoring is a process that is developed and used to review all the information obtained about the clients with whom there is the presence of a business relationship in order to:

- Detect any suspicious transactions that are required to be reported to FINTRAC;
- Keep [client identification information](#), beneficial ownership information, and the purpose and intended nature of the business relationship record up to date;
- Reassess the level of risk associated with the client's transactions and activities and
- Determine whether transactions or activities are consistent with the client information obtained and the risk assessment conducted on the client.

For more guidance on when an MB enters a business relationship, see the section on Business Relationship requirements. The MB will either monitor an individual client or a group of clients. Monitoring of a client must occur when the MB enters into a business relationship with the client. The monitoring must be conducted periodically based on the risk assessment of the client. As an example, clients that are risk-rated low may require less ongoing monitoring, while clients that are in the high-risk category require enhanced measures and enhanced monitoring. For further information on the frequency of monitoring, refer to the procedures.

9.5.6.1 Enhanced Monitoring

Where a client is identified as high-risk, enhanced measures and enhanced monitoring of a client that has been identified as high-risk must be undertaken. Enhanced ongoing monitoring may include:

- Reviewing transactions based on an approved schedule that involves management sign-off;
- Developing reports and reviewing these reports of high-risk transactions more frequently;
- Flagging certain activities or those that deviate from the MB's expectations and raise concerns, as necessary;
- Setting business limits or parameters on accounts or transactions that would trigger early warning signals and require a mandatory review or
- Reviewing transactions more frequently against suspicious transaction indicators relevant to business relationships.

9.5.6.2 Ongoing Monitoring-Record Keeping

Records must be kept of the measures undertaken to conduct ongoing monitoring and the information obtained from the ongoing monitoring of business relationships. This includes:

- The processes in place to perform ongoing monitoring;
- The processes in place to perform the enhanced ongoing monitoring of high-risk clients;
- The processes for recording the information obtained because of ongoing monitoring;
- The processes for recording the information obtained because of enhanced ongoing monitoring of high-risk clients and
- The information was obtained due to ongoing monitoring and enhanced ongoing monitoring of high-risk clients.

The procedures document details regarding the measures used to conduct ongoing monitoring of businesses. The information obtained because of the ongoing monitoring will be captured in a separate record. The process of documenting those results is recorded in the Procedure.

The record of ongoing monitoring measures taken and the information obtained from that ongoing monitoring is retained for at least five years from the date the record was

created.

9.5.6.3 Enhanced Monitoring-Cease

Enhanced monitoring ceases when the business relationship ends or when, after reassessing the risk related to the client, they are no longer considered high-risk. Although enhanced monitoring measures cease based on the client's risk assessment, ongoing monitoring continues to be conducted.

9.5.7 Third-Party Determination

A third party is a person or entity that instructs another person or entity to conduct a transaction or activity on their behalf. As such, the third party is the instructing party to the transaction or activity and is also understood as the "on behalf of" party.

Reasonable measures must be taken to determine whether a third party is involved when carrying out certain transactions or activities. Reasonable measures for third-party determination could include asking the client if they are acting at the instruction of another person or entity or whether another person or entity will be instructing on the account. The steps taken as reasonable measures to make a third-party determination are documented in the procedures.

Third-party determination is required when there is a need to:

- report a large cash transaction or keep a large cash transaction record;
- report a large virtual currency transaction and keep a record or;
- keep an information record.

When cash is received in the amount of \$10,000 CAD or more and is therefore reportable to FINTRAC, or where a large cash transaction record is required to be kept, the MB must take reasonable measures to determine whether the person who gave the cash is acting on behalf of a third party.

When receiving an amount in virtual currency equivalent to \$10,000 CAD or more and is therefore reportable to FINTRAC, or when a large virtual currency transaction record is required to be kept, reasonable measures must be taken by the MB to determine whether the person from whom provided the virtual currency is acting on behalf of a third party.

9.5.8 Information Record

As an MB, you are required to keep an information record for certain transactions or activities. When an information record is created, reasonable measures must be taken to determine whether the person or entity for which it is kept is acting on behalf of a third party.

9.5.9 Actual Third-Party Involvement

If the MB has determined that there is third-party involvement:

- If the third party is a person—their name, address, telephone number (not required if the third-party determination is made for a large cash transaction or large VC transaction), date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business;
- If the third party is a corporation or another entity—its name, address, telephone number (not required if the third-party determination is made for a large cash transaction or large VC transaction), the nature of its principal business, its registration or incorporation number and the jurisdiction (province or state) and country of issue of that number; and
- the relationship between the third party and the following person or entity, as applicable:
 - The person who conducts the large cash transaction;
 - The person who conducts the large VC transaction;
 - The account holder(s);
 - The person or entity that the information record is kept on; or
 - The person or entity that requests the casino disbursement.

A record of the information obtained must be kept. The information, as a result of the third-party determination, helps complete the “on behalf of” section of any respective FINTRAC report submission. If the MB is unable to make a third-party determination but suspects that a third party is involved, a record must be kept:

- Describing why the person or entity is acting on behalf of a third party;
- The record is required to include:
 - When \$10,000 or more CAD was received in cash (resulting in an LCTR and a large cash transaction record), whether the person who provided the cash disclosed they were acting on behalf of a third party

- When \$10,000 or more CAD was received in virtual currency (resulting in an LVCTR and a large virtual currency transaction record), whether the person who provided the virtual currency disclosed they were acting on behalf of a third party
- When creating an information record, whether the person or entity for which the information record is being kept states whether they are acting on their own behalf only.

All records must be kept for five years from the record's creation date.

For examples of third-party records, please see the [link](#) to Annex 1 in the section on Third-Party Determination section.

9.6 Politically Exposed Persons (PEP)

Reasonable measures must be taken to determine whether the MB is dealing with the following people:

- A politically exposed domestic person (“PEP”);
- A politically exposed foreign person (determination conducted in specific circumstances, “foreign PEP”);
- A head of an international organization (“HIO”);
- A family member of a person who is closely associated with one of those persons;
- A close associate of one of those persons (for the cash or virtual currency transaction or if a fact is detected related to a business relationship);
- A close associate of a politically exposed foreign person (for business relationships).

MB must take reasonable measures to perform a determination when:

- (1) Entering into a business relationship;
- (2) Conduct periodic monitoring of the business relationship;
- (3) Detect a fact about the business relationship that indicated a PEP or HIO connection,

From a transactional perspective, a Mortgage Broker must also conduct a determination when:

- (4) In receipt of an amount of CAD 100,000 or more in cash or virtual currency.

9.6.1 Business Relationship Related-PEP or HIO Determination

Reasonable measures must be taken to determine whether a person is a PEP, HIO, family member or a close associate of a foreign PEP when entering into a business relationship.

9.6.2 Periodic Monitoring of Business Relationships-PEP or HIO Determination

As part of the periodic monitoring, reasonable measures must be taken to determine whether a person the MB is entering into a business relationship with is a PEP, HIO, family member of one of those persons, or close associate of a foreign PEP.

9.6.3 Detect A Fact About Existing Business Relationship-PEP or HIO Determination

Suppose the MB detects a fact that constitutes reasonable grounds to suspect that a person with whom the Mortgage have a business relationship is a PEP, HIO, or family member or close associate of one of these persons. In that case, the MB must take reasonable measures to determine whether they are such a person.

9.6.4 Receipt of an amount of \$100,000 or more in cash or an amount of VC equivalent to CAD 100,000 or more

The MB must take reasonable measures to determine whether a person from whom they receive CAD 100,000 or more in cash or virtual currency is a PEP, HIO, family member, or close associate of one of these persons.

A PEP or family member determination does not need to be conducted if the MB has already determined that a person is a foreign PEP or a family member of a foreign PEP.

9.6.5 Measures to be Taken After Making a PEP, HIO, Family Member or Close Associate Determination-Business Relationship Related Measures

9.6.5.1 Foreign PEPs

When the MB enters a business relationship, conducts periodic monitoring of business relationships, or detects a fact about an existing business relationship, and determines that a person is a foreign PEP or family member or close associate of a foreign PEP, the MB must:

- Take reasonable measures to establish the person's source of wealth and
- Take [enhanced measures](#), including taking additional measures to verify the person's identity, conducting enhanced ongoing monitoring of the business

relationship, and taking any other enhanced measures to mitigate the risks the person poses.

Note: Enhanced measures must be taken when a foreign PEP determination is made.

9.6.5.2 Domestic PEPs or HIOs

When the MB enters a business relationship, conducts periodic monitoring of business relationships, detects a fact about an existing business relationship, and determines that a person is a domestic PEP, HIO, or family member of a domestic PEP or HIO. Based on the MB risk assessment, there is a high risk of a money laundering or terrorist activity offence being committed; the MB must:

- Take reasonable measures to establish the person's source of wealth and
- Take enhanced measures, including taking additional measures to verify the person's identity, conducting enhanced ongoing monitoring of the business relationship, and taking any other enhanced measures to mitigate the risks posed by the person.

When the MB detect a fact about an existing business relationship and determines that a person is a close associate of a domestic PEP or HIO, and based on the MB's risk assessment, there is a high risk of a money laundering or terrorist activity offence being committed, the MB must:

- Take reasonable measures to establish the person's source of wealth and

Take enhanced measures, including taking additional measures to verify the person's identity, conducting enhanced ongoing monitoring of the business relationship, and taking any other enhanced measures to mitigate the risks posed by the person.

9.6.6 Prescribed Timing for Taking Measures-Business Relationship

When the MB enters into a business relationship with, **detects a fact** about a PEP, HIO, or family member or close associate of one of these persons, the MB has 30 days after the day on which the business relationship was entered into or detected a fact to take reasonable measures to establish the source of a person's wealth.

9.6.7 Measures to be Taken After Making a PEP, HIO, Family Member or Close Associate Determination-Transaction Related Measures

9.6.7.1 Foreign PEPs

When the MB receives an amount of \$100,000 or more in cash or an amount of VC equivalent to \$100,000 or more and determines that a person is a foreign PEP or family member or close associate of a foreign PEP, the MB must:

- Take reasonable measures to establish the source of the cash or source of the VC used for the transaction and the source of the person's wealth and
- Ensure that a member of senior management reviews the transaction.

9.6.7.2 Domestic PEPs or HIOs

When the MB receives an amount of \$100,000 or more in cash or an amount of VC equivalent to \$100,000 or more and determines that the person is a domestic PEP, HIO, or family member or close associate of a domestic PEP or HIO, and based on the MB risk assessment consider there to be a high-risk of a money laundering or terrorist financing offence being committed, the MB must:

- Take reasonable measures to establish the source of the funds or source of the VC used for the transaction and to establish the source of the person's wealth and
- Ensure that a member of senior management reviews the transaction.

9.6.7.3 Prescribe Timing for Taking Measures-Transactional

When the MB has received an amount of \$100,000 or more in cash or an amount of VC equivalent to \$100,000 or more, a determination must be made within 30 days after the day on which the transaction is conducted to:

- Take reasonable measures to make a PEP, HIO, family member, or close associate determination;
- Suppose the MB determines the person is a PEP, HIO, or close associate or family member of a PEP or HIO. In that case, they must take reasonable measures to establish the source of the cash or virtual currency used for the transaction, establish the person's source of wealth, and ensure that a member of senior management reviews the transaction.

9.6.7.4 Records To Be Kept: PEP, HIOs, Family Member or Close Associates

9.6.7.5 PEP and HIO Business Relationship Records

When an MB enter into a business relationship, conducts periodic monitoring of business relationships, or detects a fact about an existing business relationship, and determines that the person is a PEP, HIO, or a family member or close associate of one of those persons, a record must be kept of:

- The office or position and the name of the organization or institution of the PEP or HIO;
- The date of the determination and
- The source of the person's wealth, if known.

The MB must keep PEP and HIO business relationship records for at least five years after the day on which they were created.

9.6.7.6 PEP and HIO Transaction Records

The MB must keep a record of the PEP HIO determinations that were conducted when, as a result, the MB was in receipt of an **amount of \$100,000 or more in cash or an amount of VC equivalent to \$100,000 or more**. PEP and HIO transactional-based determinations must be conducted in accordance with the previous section. The following records must be kept:

- The office or position and the name of the organization or institution of the PEP or HIO;
- The date of the determination;
- The source of the cash or source of the VC used for the transaction if known;
- The source of the person's wealth, if known;
- The name of the member of senior management who reviewed the transaction; and
- The date of that review.

In the case of family members and close associates of PEPs and HIOs, the record of the nature of the relationship between the person and the PEP or HIO, is required to be recorded.

Retention: The MB must keep all requisite PEP and HIO determination records listed above and the transactional record qualifying the transactions for a PEP HIO determination. The records must be kept for at least five years after the day they were created.

10. Ministerial Directives and Transaction Restriction

Under Part 1.1 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), which came into force on June 19, 2014, the Minister of Finance may:

- Issue directives that require reporting entities to apply countermeasures to transactions coming from or going to designated foreign jurisdictions or entities and
- Recommend the introduction of regulations to restrict reporting entities from entering into a financial transaction coming from or going to designated foreign jurisdictions or entities.

These authorities allow the Minister of Finance to take steps to protect Canada's financial system from foreign jurisdictions and foreign entities that are considered to present high risks for facilitating money laundering and terrorist financing.

10.1 Ministerial directives

The directive will be issued by the Minister of Finance, and FINTRAC will inform MBs that it has been issued. Each directive includes an outline of countermeasures limited to the same activities for which reporting entities already have obligations. The countermeasures will enhance or add to these obligations.

Directives will specify the date they come into force and will remain in force until officially revoked, suspended or amended.

Directives will be reviewed at least every three years from the day they take effect.

Directives in force:

- [February 24, 2024: Russia](#)
- [July 25, 2020: Islamic Republic of Iran](#) Updated February 24, 2024
- [December 9, 2017: Democratic People's Republic of Korea \(DPRK\)](#)

10.2 Compliance with Ministerial Directives and Transaction Restrictions

FINTRAC will monitor and assess MB's compliance with the directives listed above. FINTRAC has the authority, through the PCMLTFA, to examine the MB's records and inquire into business affairs. As part of an onsite or desk examination, FINTRAC will review how MBs comply with their obligations, including directives under the PCMLTFA.

FINTRAC may issue administrative monetary penalties (AMPs) to address non-compliance and may use other enforcement tools available under the PCMLTFA. The AMP framework was materially amended effective March 26, 2026.

For prescribed violations occurring on or after March 26, 2026, the applicable Regulations provide penalty ranges of \$1 to \$40,000 for a minor violation, \$1 to \$4,000,000 for a serious violation, and \$1 to \$20,000,000 for a very serious violation, subject to the statutory maximums and other applicable provisions of the PCMLTFA.

For prescribed violations, the maximum penalty is \$4,000,000 if committed by a person and \$20,000,000 if committed by an entity. For all prescribed violations identified on a notice of violation taken together, the statutory maximum is the greater of \$4,000,000 or 3% of gross global income for a person, and the greater of \$20,000,000 or 3% of gross global revenue for an entity, as applicable under the PCMLTFA.

- The amended framework also introduces mandatory compliance agreements for prescribed violations and compliance orders as an additional enforcement tool. Criminal offence provisions remain separate from the AMP regime and must not be treated as interchangeable with administrative penalties.
- The Compliance Officer must consult the current PCMLTFA, Regulations and FINTRAC AMP guidance when assessing potential non-compliance, because violation classifications, penalty calculations and enforcement processes may be amended or supplemented by regulation or guidance.

Where the same act or omission may be proceeded with as a violation or as an offence, proceeding in one manner precludes proceeding in the other, in accordance with the PCMLTFA.

1. Appendix 1: Definitions

Below is a summary and list of definitions for words used throughout the above Policy document. The information has been taken from the glossary of definitions found on the FINTRAC website. For an electronic copy, please see the [link](#).

1.1. Accountant

A chartered accountant, a certified general accountant, a certified management accountant or, if applicable, a chartered professional accountant. (comptable)

Reference:

Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), SOR/2002-184, s. 1(2).

1.2. Accounting firm

An entity that is engaged in the business of providing accounting services to the public and has at least one partner, employee or administrator that is an accountant. (cabinet d'expertise comptable)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.3. Act

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). (la Loi)

Reference:

Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (PCMLTFAMPR), SOR/2007-292, s. 1,

Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations (PCMLTFRR), SOR/2007-121, s. 1, PCMLTFR, SOR/2002-184, s. 1(2), and

Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (PCMLTFSTRR), SOR/2001-317, s. 1(2).

1.4. Administrative monetary penalties (AMPs)

Civil penalties that may be issued to reporting entities by FINTRAC for non-compliance with the PCMLTFA and associated Regulations. (pénalité administrative pécuniaire [PAP])

1.5. Affiliate

An entity is affiliated with another entity if one of them is wholly owned by the other, if both are wholly owned by the same entity or if their financial statements are consolidated. (entité du même groupe)

Reference:
PCMLTFR, SOR/2002-184, s. 4.

1.6. Annuity

Has the same meaning as in subsection 248(1) of the [Income Tax Act](#). (rente)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.7. Armoured cars

Persons or entities that are engaged in the business of transporting currency, money orders, traveller's cheques or other similar negotiable instruments. (Véhicules blindés)

1.8. As soon as practicable

A time period that falls in-between immediately and as soon as possible, within which a STR (STR) must be submitted to FINTRAC. The completion and submission of the STR should take priority over other tasks. In this context, the report must be completed promptly, taking into account the facts and circumstances of the situation. While some delay is permitted, it must have a reasonable explanation. (aussitôt que possible)

1.9. Attempted transaction

Occurs when an individual or entity starts to conduct a transaction that is not completed. For example, a client or a potential client walks away from conducting a \$10,000 cash deposit. (opération tentée)

1.10. Authentic

In respect of verifying identity, means genuine and having the character of an original, credible, and reliable document or record. (authentique)

1.11. Authorized person

A person who is authorized under subsection 45(2). (personne autorisée)

Reference:
Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), S.C. 2000, c 17, s. 2(1).

1.12. Authorized user

A person who is authorized by a holder of a prepaid payment product account to have electronic access to funds or virtual currency available in the account by means of a prepaid payment product that is connected to it. (utilisateur autorisé)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.13. Beneficial owner(s)

Beneficial owners are the individuals who are the trustees, and known beneficiaries and settlors of a trust, or who directly or indirectly own or control 25% or more of i) the shares of a corporation or ii) an entity other than a corporation or trust, such as a partnership. The ultimate beneficial owner(s) cannot be another corporation or entity; it must be the actual individual(s) who owns or controls the entity. (bénéficiaire effectif)

1.14. Beneficiary

A beneficiary is the individual or entity that will benefit from a transaction or to which the final remittance is made. (bénéficiaire)

1.15. Branch

A branch is a part of your business at a distinct location other than your main office. (succursale)

1.16. British Columbia notary corporation

An entity that carries on the business of providing notary services to the public in British Columbia in accordance with the Notaries Act, R.S.B.C. 1996, c. 334. (société de notaires de la Colombie-Britannique)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.17. British Columbia notary public

A person who is a member of the Society of Notaries Public of British Columbia. (notaire public de la Colombie-Britannique)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.18. Cash

Coins referred to in section 7 of the Currency Act, notes issued by the Bank of Canada under the Bank of Canada Act that are intended for circulation in Canada or coins or bank notes of countries other than Canada. (espèces)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2) and PCMLTFSTR, SOR/2001-317, s. 1(2).

1.19. Casino

A government, organization, board or operator that is referred to in any of paragraphs 5(k) to (k.3) of the Act. (casino)

Reference:

PCMLTFR, SOR/2002-184, s 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

1.20. Certified translator

An individual that holds the title of professional certified translator granted by a Canadian provincial or territorial association or body that is competent under Canadian provincial or territorial law to issue such certification. (traducteur agréé)

1.21. Clarification request

A clarification request is a method used to communicate with money services businesses (MSBs) or foreign money services businesses (FMSBs) when FINTRAC needs more information about their registration form. This request is usually sent by email. (demande de précisions)

1.22. Client

A person or entity that engages in a financial transaction with another person or entity. (client)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.23. Client identification information

The identifying information that you have obtained on your clients, such as name, address, telephone number, occupation or nature of principal business, and date of birth for an individual. (renseignements d'identification du client)

1.24. Competent authority

For the purpose of the criminal record check submitted with an application for registration, a competent authority is any person or organization that has the legally delegated or invested authority, capacity, or power to issue criminal record checks. (autorité compétente)

1.25. Completed transaction

Is a transaction conducted by a person or entity, that is completed and results in the movement of funds, virtual currency, or the purchase or sale of an asset. (opération effectuée)

1.26. Completing action

With respect to a reportable transaction, information related to the instructions provided by the person or entity making the request to the reporting entity to complete a transaction. For example, an individual arrives at a bank and requests to purchase a bank draft. The completing action is the details of how the reporting entity fulfilled the person or entity's instructions which led to the transaction being completed. This includes what the funds or virtual currency initially brought to the reporting entity was used for (see "disposition"). A transaction may have one or more completing actions depending on the instructions provided by the person or entity. (action d'achèvement)

1.27. CO

The individual, with the necessary authority, that you appoint to be responsible for the implementation of your compliance program. (broker de conformité)

1.28. Compliance policies and procedures

Written methodology outlining the obligations applicable to your business under the PCMLTFA and its associated Regulations and the corresponding processes and controls you put in place to address your obligations. (politiques et procédures de conformité)

1.29. Compliance program

All elements (CO, policies and procedures, risk assessment, training program, effectiveness review) that you, as a reporting entity, are legally required to have under the PCMLTFA and its associated Regulations to ensure that you meet all your obligations. (programme de conformité)

1.30. Context

Clarifies a set of circumstances or provides an explanation of a situation or financial transaction that can be understood and assessed. (contexte)

1.31. Correspondent banking relationship

A relationship created by an agreement or arrangement under which an entity referred to in any of paragraphs 5(a), (b), (d),(e) and (e.1) or an entity that is referred to in section 5 and that is prescribed undertakes to provide to a prescribed foreign entity prescribed services or international electronic funds transfers, cash management or cheque clearing services. (relation de correspondant bancaire)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 9.4(3) and PCMLTFR, SOR/2002-184, s. 16(1)(b).

1.32. Country of residence

The country where an individual has lived continuously for 12 months or more. The individual must have a dwelling in the country concerned. For greater certainty, a

person only has one country of residence no matter how many dwelling places they may have, inside or outside of that country. (pays de résidence)

1.33. Credit card acquiring business

A credit card acquiring business is a financial entity that has an agreement with a merchant to provide the following services:

- enabling a merchant to accept credit card payments by cardholders for goods and services and to receive payments for credit card purchases;
- processing services, payment settlements and providing point-of-sale equipment (such as computer terminals); and
- providing other ancillary services to the merchant.

(entreprise d'acquisition de cartes de crédit)

1.34. Credit union central

A central cooperative credit society, as defined in section 2 of the [Cooperative Credit Associations Act](#), or a credit union central or a federation of credit unions or caisses populaires that is regulated by a provincial Act other than one enacted by the legislature of Quebec. (centrale de caisses de crédit)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.35. Crowdfunding platform

A website or an application or other software that is used to raise funds or virtual currency through donations. (plateforme de sociofinancement)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.36. Crowdfunding platform services

The provision and maintenance of a crowdfunding platform for use by other persons or entities to raise funds or virtual currency for themselves or for persons or entities specified by them. (services de plateforme de sociofinancement)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.37. Current

In respect of a document or source of information that is used to verify identity, is up to date, and, in the case of a government-issued photo identification document, must not have been expired when the ID was verified. (à jour)

1.38. Dealer in precious metals and stones

A person or entity that, in the course of their business activities, buys or sells precious metals, precious stones or jewellery. It includes a department or a broker of His Majesty in right of Canada or a broker or mandatary of His Majesty in right of

a province when the department or the broker or mandatary carries out the activity, referred to in subsection 65(1), of selling precious metals to the public. (négociant en métaux précieux et pierres précieuses)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.39. Deferred profit sharing plan

Has the same meaning as in subsection 248(1) of the [Income Tax Act](#). (régime de participation différée aux bénéfices)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.40. Deposit slip

A record that sets out:

1. (a) the date of the deposit;
2. (b) the name of the person or entity that makes the deposit;
3. (c) the amount of the deposit and of any part of it that is made in cash;
4. (d) the method by which the deposit is made; and
5. (e) the number of the account into which the deposit is made and the name of each account holder.

(relevé de dépôt)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.41. Directing services

A business is directing services at persons or entities in Canada if at least one of the following applies:

- The business's marketing or advertising is directed at persons or entities located in Canada;
- The business operates a ".ca" domain name; or,
- The business is listed in a Canadian business directory.

Additional criteria may be considered, such as if the business describes its services being offered in Canada or actively seeks feedback from persons or entities in Canada. (diriger des services)

1.42. Distributed ledger

For the purpose of section 151 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), a digital ledger that is maintained by

multiple persons or entities and that can only be modified by a consensus of those persons or entities. (registres distribués)

Reference:
PCMLTFR, SOR/2002-184, s. 151(2).

1.43. Disposition

With respect to a reportable transaction, the disposition is what the funds or virtual currency was used for. For example, an individual arrives at a bank with cash and purchases a bank draft. The disposition is the purchase of the bank draft. (répartition)

1.44. Electronic funds transfer

The transmission—by any electronic, magnetic or optical means—of instructions for the transfer of funds, including a transmission of instructions that is initiated and finally received by the same person or entity. In the case of SWIFT messages, only SWIFT MT-103 messages and their equivalent are included. It does not include a transmission or instructions for the transfer of funds:

1. (a) that involves the beneficiary withdrawing cash from their account;
2. (b) that is carried out by means of a direct deposit or pre-authorized debit;
3. (c) that is carried out by cheque imaging and presentment
4. (d) that is both initiated and finally received by persons or entities that are acting to clear or settle payment obligations between themselves; or
5. (e) that is initiated or finally received by a person or entity referred to in paragraphs 5(a) to (h.1) of the Act for the purpose of internal treasury management, including the management of their financial assets and liabilities, if one of the parties to the transaction is a subsidiary of the other or if they are subsidiaries of the same corporation.

(télévirement)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.45. Employees profit sharing plan

Has the same meaning as in subsection 248(1) of the [Income Tax Act](#). (régime de participation des employés aux bénéfices)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.46. Entity

A body corporate, a trust, a partnership, a fund or an unincorporated association or organization. (entité)

Reference:
PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.47. Facts

Actual events, actions, occurrences or elements that exist or are known to have happened or existed. Facts are not opinions. For example, facts surrounding a transaction or multiple transactions could include the date, time, location, amount or type of transaction or could include the account details, particular business lines, or the client's financial history. (faits)

1.48. Family member

For the purposes of subsection 9.3(1) of the Act, a prescribed family member of a politically exposed foreign person, a politically exposed domestic person or a head of an international organization is:

1. (a) their spouse or common-law partner;
2. (b) their child;
3. (c) their mother or father;
4. (d) the mother or father of their spouse or common-law partner; or
5. (e) a child of their mother or father.

(membre de la famille)

Reference:
PCMLTFR, SOR/2002-184, s. 2(1).

1.49. Fiat currency

A currency that is issued by a country and is designated as legal tender in that country. (monnaie fiduciaire)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2) and PCMLTFSTR, SOR/2001-317, s. 1(2).

1.50. Final receipt

In respect of an electronic funds transfer, means the receipt of the instructions by the person or entity that is to make the remittance to a beneficiary. (destinataire)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.51. Financial entity

Means:

1. (a) an entity that is referred to in any of paragraphs 5(a), (b) and (d) to (f) of the Act;

2. (b) a financial services cooperative;
3. (c) a life insurance company, or an entity that is a life insurance broker or broker, in respect of loans or prepaid payment products that it offers to the public and accounts that it maintains with respect to those loans or prepaid payment products, other than:
 1. (i) loans that are made by the insurer to a policy holder if the insured person has a terminal illness that significantly reduces their life expectancy and the loan is secured by the value of an insurance policy;
 2. (ii) loans that are made by the insurer to the policy holder for the sole purpose of funding the life insurance policy; and
 3. (iii) advance payments to which the policy holder is entitled that are made to them by the insurer;
4. (d) a credit union central when it offers financial services to a person, or to an entity that is not a member of that credit union central; and
5. (e) a department, or an entity that is a broker of His Majesty in right of Canada or a broker or mandatary of His Majesty in right of a province, when it carries out an activity referred to in section 76.

(entité financière)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.52. Financial Action Task Force

The Financial Action Task Force on Money Laundering established in 1989.
(Groupe d'action financière)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.53. Financial services cooperative

A financial services cooperative that is regulated by an Act respecting financial services cooperatives, CQLR, c. C-67.3, other than a caisse populaire.
(coopérative de services financiers)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.54. Foreign currency

A fiat currency that is issued by a country other than Canada. (devise)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.55. Foreign currency exchange transaction

An exchange, at the request of another person or entity, of one fiat currency for another. (opération de change en devise)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.56. Foreign currency exchange transaction ticket

A record respecting a foreign currency exchange transaction—including an entry in a transaction register—that sets out:

1. (a) the date of the transaction;
2. (b) in the case of a transaction of \$3,000 or more, the name and address of the person or entity that requests the exchange, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
3. (c) the type and amount of each of the fiat currencies involved in the payment made and received by the person or entity that requests the exchange;
4. (d) the method by which the payment is made and received;
5. (e) the exchange rates used and their source;
6. (f) the number of every account that is affected by the transaction, the type of account and the name of each account holder; and
7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number.

(fiche d'opération de change en devise)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.57. Foreign money services business

Persons and entities that do not have a place of business in Canada, that are engaged in the business of providing at least one of the following services that is directed at persons or entities in Canada, and that provide those services to their clients in Canada:

1. (i) foreign exchange dealing,
2. (ii) remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,
3. (iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity,
4. (iv) dealing in virtual currencies, or
5. (v) any prescribed service.

(entreprise de services monétaires étrangère)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 5(h.1), PCMLTFRR, SOR/2007-121, s. 1 and PCMLTFR, SOR/2002-184, s. 1(2).

1.58. Foreign state

Except for the purposes of Part 2, means a country other than Canada and includes any political subdivision or territory of a foreign state. (État étranger)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.59. Funds

Means:

1. (a) cash and other fiat currencies, and securities, negotiable instruments or other financial instruments that indicate a title or right to or interest in them; or
2. (b) a private key of a cryptographic system that enables a person or entity to have access to a fiat currency other than cash.

For greater certainty, it does not include virtual currency. (fonds)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

1.60. Head of an international organization

A person who, at a given time, holds—or has held within a prescribed period before that time—the office or position of head of

1. a) an international organization that is established by the governments of states;
2. b) an institution of an organization referred to in paragraph (a); or
3. c) an international sports organization.

(dirigeant d'une organisation internationale)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 9.3(3).

1.61. Immediately

In respect of submitting a Listed Person or Entity Property Report (LPEPR), the time period within which the report must be submitted, which does not allow for any delay prior to submission. (immédiatement)

1.62. Information record

A record that sets out the name and address of a person or entity and:

1. (a) in the case of a person, their date of birth and the nature of their principal business or their occupation; and
2. (b) in the case of an entity, the nature of its principal business.

(dossier de renseignements)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.63. Initiation

In respect of an electronic funds transfer, means the first transmission of the instructions for the transfer of funds. (amorcer)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.64. Institutional trust

For the purpose of section 15 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), means a trust that is established by a corporation or other entity for a particular business purpose and includes a pension plan trust, a pension master trust, a supplemental pension plan trust, a mutual fund trust, a pooled fund trust, a registered retirement savings plan trust, a registered retirement income fund trust, a registered education savings plan trust, a group registered retirement savings plan trust, a deferred profit sharing plan trust, an employee profit sharing plan trust, a retirement compensation arrangement trust, an employee savings plan trust, a health and welfare trust, an unemployment benefit plan trust, a foreign insurance company trust, a foreign reinsurance trust, a reinsurance trust, a real estate investment trust, an environmental trust and a trust established in respect of endowment, a foundation or a registered charity. (fiducie institutionnelle)

Reference:

PCMLTFR, SOR/2002-184, s. 15(2).

1.65. International electronic funds transfer

An electronic funds transfer other than for the transfer of funds within Canada. (télévirement international)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.66. Inter vivos trust

A personal trust, other than a trust created by will. (fiducie entre vifs)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.67. Jewellery

Objects that are made of gold, silver, palladium, platinum, pearls or precious stones and that are intended to be worn as a personal adornment. (bijou)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.68. Large cash transaction record

A record that indicates the receipt of an amount of \$10,000 or more in cash in a single transaction and that contains the following information:

1. (a) the date of the receipt;
2. (b) if the amount is received for deposit into an account, the number of the account, the name of each account holder and the time of the deposit or an indication that the deposit is made in a night deposit box outside the recipient's normal business hours;
3. (c) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
4. (d) the type and amount of each fiat currency involved in the receipt;
5. (e) the method by which the cash is received;
6. (f) if applicable, the exchange rates used and their source;
7. (g) the number of every other account that is affected by the transaction, the type of account and the name of each account holder
8. (h) every reference number that is connected to the transaction and has a function equivalent to that of an account number;
9. (i) the purpose of the transaction;
10. (j) the following details of the remittance of, or in exchange for, the cash received:
 1. (i) the method of remittance;
 2. (ii) if the remittance is in funds, the type and amount of each type of funds involved;
 3. (iii) if the remittance is not in funds, the type of remittance and its value, if different from the amount of cash received; and
 4. (iv) the name of every person or entity involved in the remittance and their account number or policy number or, if they have no account number or policy number, their identifying number; and
11. (k) if the amount is received by a dealer in precious metals and precious stones for the sale of precious metals, precious stones or jewellery:
 1. (i) the type of precious metals, precious stones or jewellery;

2. (ii) the value of the precious metals, precious stones or jewellery, if different from the amount of cash received, and
3. (iii) the wholesale value of the precious metals, precious stones or jewellery.

(relevé d'opération importante en espèces)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.69. Large virtual currency transaction record

A record that indicates the receipt of an amount of \$10,000 or more in virtual currency in a single transaction and that contains the following information:

1. (a) the date of the receipt;
2. (b) if the amount is received for deposit into an account, the name of each account holder;
3. (c) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
4. (d) the type and amount of each virtual currency involved in the receipt;
5. (e) the exchange rates used and their source;
6. (f) the number of every other account that is affected by the transaction, the type of account and the name of each account holder;
7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number;
8. (h) every transaction identifier, including the sending and receiving addresses; and
9. (i) if the amount is received by a dealer in precious metals and precious stones for the sale of precious metals, precious stones or jewellery:
 1. (i) the type of precious metals, precious stones or jewellery;
 2. (ii) the value of the precious metals, precious stones or jewellery, if different from the amount of virtual currency received; and
 3. (iii) the wholesale value of the precious metals, precious stones or jewellery.

(relevé d'opération importante en monnaie virtuelle)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.70. Life insurance broker or agent

A person or entity that is authorized under provincial legislation to carry on the business of arranging contracts of life insurance. (représentant d'assurance-vie)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.71. Life insurance company

A life company or foreign life company to which the [Insurance Companies Act](#) applies or a life insurance company regulated by a provincial Act. (société d'assurance-vie)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.72. Listed person

Has the same meaning as in section 1 of the [Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism](#). (personne inscrite)

Reference:
PCMLTFSTRR, SOR/2001-317, s. 1(2).

1.73. Managing general agents (MGAs)

Life insurance brokers or agents that act as facilitators between other life insurance brokers or agents and life insurance companies. MGAs typically offer services to assist with insurance agents contracting and commission payments, facilitate the flow of information between insurer and agent, and provide training to, and compliance oversight of, insurance agents. (agent général de gestion)

1.74. Mandatary

A person who acts, under a mandate or agreement, for another person or entity. (mandataire)

1.75. Marketing or advertising

When a person or entity uses promotional materials such as advertisements, graphics for websites or billboards, etc., with the intent to promote money services business (MSB) services and to acquire business from persons or entities in Canada. (marketing ou publicité)

1.76. Minister

In relation to sections 24.1 to 39, the Minister of Public Safety and Emergency Preparedness and, in relation to any other provision of this Act, the Minister of Finance. (ministre)

Reference:
PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.77. Money laundering offence

An offence under subsection 462.31(1) of the [Criminal Code](#). The United Nations defines money laundering as "any act or attempted act to disguise the source of money or assets derived from criminal activity." Essentially, money laundering is the process whereby "dirty money"—produced through criminal activity—is transformed into "clean money," the criminal origin of which is difficult to trace. (infraction de recyclage des produits de la criminalité)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.78. Money laundering and terrorist financing indicators (ML/TF indicators)

Potential red flags that could initiate suspicion or indicate that something may be unusual in the absence of a reasonable explanation. [Indicateurs de blanchiment d'argent (BA) et de financement du terrorisme (FT) (indicateurs de BA/FT)]

1.79. Money services business

A person or entity that has a place of business in Canada and that is engaged in the business of providing at least one of the following services:

1. (i) foreign exchange dealing,
2. (ii) remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,
3. (iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity,
4. (iv) dealing in virtual currencies, or
5. (v) any prescribed service.

(entreprise de services monétaires)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 5(h), PCMLTFRR, SOR/2007-121, s. 1 and PCMLTFR, SOR/2002-184, s. 1(2).

1.80. Money services business agent

An individual or entity authorized to deliver services on behalf of a money services business (MSB). It is not an MSB branch. (mandataire d'une entreprise de services monétaires)

1.81. Nature of principal business

An entity's type or field of business. Also applies to an individual in the case of a sole proprietorship. (nature de l'entreprise principale)

1.82. New developments

Changes to the structure or operations of a business when new services, activities, or locations are put in place. For example, changes to a business model or business restructuring. (nouveaux développements)

1.83. New technologies

The adoption of a technology that is new to a business. For example, when a business adopts new systems or software such as transaction monitoring systems or client onboarding and identification tools. (nouvelles technologies)

1.84. No apparent reason

There is no clear explanation to account for suspicious behaviour or information. (sans raison apparente)

1.85. Occupation

The job or profession of an individual. (profession ou métier)

1.86. Person

An individual. (personne)

Reference:
PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.87. Person authorized to give instructions

In respect of an account, means a person who is authorized to instruct on the account or make changes to the account, such as modifying the account type, updating the account contact details, and in the case of a credit card account, requesting a limit increase or decrease, or adding or removing card holders. A person who is only able to conduct transactions on the account is not considered a person authorized to give instructions. (personne habilitée à donner des instructions)

1.88. Politically exposed domestic person

A person who, at a given time, holds—or has held within a prescribed period before that time—one of the offices or positions referred to in any of paragraphs (a) and (c) to (j) in or on behalf of the federal government or a provincial government or any of the offices or positions referred to in paragraphs (b) and (k):

1. (a) Governor General, lieutenant governor or head of government;
2. (b) member of the Senate or House of Commons or member of a legislature of a province;
3. (c) deputy minister or equivalent rank;
4. (d) ambassador, or attaché or counsellor of an ambassador;

5. (e) military officer with a rank of general or above;
6. (f) president of a corporation that is wholly owned directly by His Majesty in right of Canada or a province;
7. (g) head of a government agency;
8. (h) judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
9. (i) leader or president of a political party represented in a legislature;
10. (j) holder of any prescribed office or position; or
11. (k) mayor, reeve or other similar chief officer of a municipal or local government.

(national politiquement vulnérable)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 9.3(3).

1.89. Politically exposed foreign person

A person who holds or has held one of the following offices or positions in or on behalf of a foreign state:

1. (a) head of state or head of government;
2. (b) member of the executive council of government or member of a legislature;
3. (c) deputy minister or equivalent rank;
4. (d) ambassador, or attaché or counsellor of an ambassador;
5. (e) military officer with a rank of general or above;
6. (f) president of a state-owned company or a state-owned bank;
7. (g) head of a government agency;
8. (h) judge of a supreme court, constitutional court or other court of last resort;
9. (i) leader or president of a political party represented in a legislature; or
10. (j) holder of any prescribed office or position.

(étranger politiquement vulnérable)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.90. Possibility

In regards to completing a STR (STR), the likelihood that a transaction may be related to a money laundering/terrorist financing (ML/TF) offence. For example, based on your assessment of facts, context and ML/TF indicators you have reasonable grounds to suspect that a transaction is related to the commission or attempted commission of an ML/TF offence. (possibilité)

1.91. Precious metal

Gold, silver, palladium or platinum in the form of coins, bars, ingots or granules or in any other similar form. (métal précieux)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.92. Precious stones

Diamonds, sapphires, emeralds, tanzanite, rubies or alexandrite. (pierre précieuse)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.93. Prepaid payment product

A product that is issued by a financial entity and that enables a person or entity to engage in a transaction by giving them electronic access to funds or virtual currency paid to a prepaid payment product account held with the financial entity in advance of the transaction. It excludes a product that:

1. (a) enables a person or entity to access a credit or debit account or one that is issued for use only with particular merchants; or
2. (b) is issued for single use for the purposes of a retail rebate program.

(produit de paiement prépayé)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.94. Prepaid payment product account

An account – other than an account to which only a public body or, if doing so for the purposes of humanitarian aid, a registered charity as defined in subsection 248(1) of the Income Tax Act, can add funds or virtual currency – that is connected to a prepaid payment product and that permits:

1. (a) funds or virtual currency that total \$1,000 or more to be added to the account within a 24-hour period; or
2. (b) a balance of funds or virtual currency of \$1,000 or more to be maintained.

(compte de produit de paiement prépayé)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.95. Prescribed

Prescribed by regulations made by the Governor in Council. (Version anglaise seulement)

Reference:
PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.96. Probability

The likelihood in regards to completing a STR (STR) that a financial transaction is related to a money laundering/terrorist financing (ML/TF) offence. For example, based on facts, having reasonable grounds to believe that a transaction is probably related to the commission or attempted commission of an ML/TF offence. (probabilité)

1.97. Production order

A judicial order that compels a person or entity to disclose records to peace officers or public officers. (ordonnance de communication)

1.98. Public body

Means

1. (a) a department or an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty in right of a province;
2. (b) an incorporated city or town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body in Canada or an agent or mandatary in Canada of any of them; and
3. (c) 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 an agent or mandatary of such an organization.

(organisme public)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.99. Real estate broker or sales representative

A person or entity that is authorized under provincial legislation to act as an agent or mandatary for purchasers or vendors in respect of the purchase or sale of real property or immovables. (courtier ou agent immobilier)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.100. Real estate developer

A person or entity that, in any calendar year after 2007, has sold to the public, other than in the capacity of a real estate broker or sales representative:

1. (a) five or more new houses or condominium units;
2. (b) one or more new commercial or industrial buildings; or
3. (c) one or more new multi-unit residential buildings each of which contains five or more residential units, or two or more new multi-unit residential buildings that together contain five or more residential units.

(promoteur immobilier)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.101. Reasonable measures

Steps taken to achieve a desired outcome, even if they do not result in the desired outcome. For example, this can include doing one or more of the following:

- asking the client,
- conducting open source searches,
- retrieving information already available, including information held in non-digital formats, or
- consulting commercially available information.

(mesures raisonnables)

1.102. Receipt of funds record

A record that indicates the receipt of an amount of funds and that contains the following information:

1. (a) the date of the receipt;
2. (b) if the amount is received from a person, their name, address and date of birth and the nature of their principal business or their occupation;
3. (c) if the amount is received from or on behalf of an entity, the entity's name and address and the nature of their principal business;
4. (d) the amount of the funds received and of any part of the funds that is received in cash;
5. (e) the method by which the amount is received;
6. (f) the type and amount of each fiat currency involved in the receipt;
7. (g) if applicable, the exchange rates used and their source;
8. (h) the number of every account that is affected by the transaction in which the receipt occurs, the type of account and the name of each account holder;

9. (i) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
10. (j) every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
11. (k) the purpose of the transaction.

(relevé de réception de fonds)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.103. Registered pension plan

Has the same meaning as in subsection 248(1) of the [Income Tax Act](#). (régime de pension agréé)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.104. Registered retirement income fund

Has the same meaning as in subsection 248(1) of the [Income Tax Act](#). (fonds enregistré de revenu de retraite)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.105. Reliable

In respect of information that is used to verify identity, means that the source is well known, reputable, and is considered one that you trust to verify the identity of the client. (fiable)

1.106. Representative for service

An individual in Canada that has been appointed by a person or entity that is a foreign money services business (FMSB), pursuant to the PCMLTFA, to receive notices and documents on behalf of the FMSB. (représentant du service)

1.107. Risk assessment

The review and documentation of potential money laundering/terrorist financing risks in order to help a business establish policies, procedures and controls to detect and mitigate these risks and their impact. (évaluation des risques)

1.108. Sanctions evasion

Sanctions evasion offence means an offence arising from the contravention of a restriction or prohibition established by an order or a regulation made under the

United Nations Act, the Special Economic Measures Act or the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law).

1.109. Securities dealer

A person or entity that is referred to in paragraph 5(g) of the Act. (courtier en valeurs mobilières)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.110. Senior officer

In respect of an entity, means:

1. (a) a director of the entity who is one of its full-time employees;
2. (b) the entity's chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, or any person who performs any of those functions; or
3. (c) any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer.

(cadre dirigeant)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.111. Service agreement

An agreement between a money services business (MSB) and an organization according to which the MSB will provide any of the following MSB services on an ongoing basis:

- money transfers;
- foreign currency exchange;
- issuing or redeeming money orders, traveller's cheques or anything similar; or
- dealing in virtual currencies.

(accord de relation commerciale)

1.112. Settlor

A settlor is an individual or entity that creates a trust with a written trust declaration. The settlor ensures that legal responsibility for the trust is given to a trustee and that the trustee is provided with a trust instrument document that explains how the trust is to be used for the beneficiaries. A settlor includes any individual or entity that contributes financially to that trust, either directly or indirectly. (constituant)

1.113. Shell bank

A foreign financial institution that:

1. (a) does not have a place of business that:
 1. (i) is located at a fixed address—where it employs one or more persons on a full-time basis and maintains operating records related to its banking activities—in a country in which it is authorized to conduct banking activities; and
 2. (ii) is subject to inspection by the regulatory authority that licensed it to conduct banking activities; and
2. (b) is not controlled by, or under common control with, a depository institution, credit union or foreign financial institution that maintains a place of business referred to in paragraph (a) in Canada or in a foreign country.

(banque fictive)

Reference:

PCMLTFR, SOR/2002-184, s. 1(1).

1.114. Signature

Includes an electronic signature or other information in electronic form that is created or adopted by a client of a person or entity referred to in section 5 of the Act and that is accepted by the person or entity as being unique to that client.
(signature)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.115. Signature card

In respect of an account, means a document that is signed by a person who is authorized to give instructions in respect of the account, or electronic data that constitutes the signature of such a person. (fiche-signature)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

1.116. Source

The issuer or provider of information or documents for verifying identification.
(source)

1.117. Source of funds or of virtual currency (VC)

The origin of the particular funds or VC used to carry out a specific transaction or to attempt to carry out a transaction. It is how the funds were acquired, not where the funds may have been transferred from. For example, the source of funds could

originate from activities or occurrences such as employment income, gifts, the sale of a large asset, criminal activity, etc. (origine des fonds ou de la monnaie virtuelle (MV))

1.118. Source of wealth

The origin of a person's total assets that can be reasonably explained, rather than what might be expected. For example, a person's wealth could originate from an accumulation of activities and occurrences such as business undertakings, family estates, previous and current employment income, investments, real estate, inheritance, lottery winnings, etc. (origine de la richesse)

1.119. Starting action

With respect to a reportable transaction, information related to the instructions provided by the person or entity making the request to the reporting entity to start a transaction. For example, an individual arrives at a bank and requests to purchase a bank draft. The starting action is the details of the instructions for the purchase which includes the funds or virtual currency that the requesting person or entity brought to the reporting entity. A transaction must have at least one starting action. (action d'amorce)

1.120. SWIFT

The Society for Worldwide Interbank Financial Telecommunication. (SWIFT)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.121. Terrorist activity

Has the same meaning as in subsection 83.01(1) of the [Criminal Code](#). (activité terroriste)

Reference:
PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.122. Terrorist activity financing offence

An offence under section 83.02, 83.03 or 83.04 of the [Criminal Code](#) or an offence under section 83.12 of the [Criminal Code](#) arising out of a contravention of section 83.08 of that Act.

A terrorist financing offence is knowingly collecting or giving property (such as money) to carry out terrorist activities. This includes the use and possession of any property to help carry out the terrorist activities. The money earned for terrorist financing can be from legal sources, such as personal donations and profits from a business or charitable organization or from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion. (infraction de financement des activités terroristes)

Reference:
PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.123. Third party

Any individual or entity that instructs another individual or entity to act on their behalf for a financial activity or transaction. (tiers)

1.124. Threats to the security of Canada

Has the same meaning as in section 2 of the [Canadian Security Intelligence Service Act](#). (menaces envers la sécurité du Canada)

Reference:
PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.125. Training program

A written and implemented program outlining the ongoing training for your employees, brokers or other individuals authorized to act on your behalf. It should contain information about all your obligations and requirements to be fulfilled under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its associated Regulations. (programme de formation)

1.126. Trust

A right of property held by one individual or entity (a trustee) for the benefit of another individual or entity (a beneficiary). (fiducie)

1.127. Trust company

A company that is referred to in any of paragraphs 5(d) to (e.1) of the Act. (société de fiducie)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.128. Trustee

A trustee is the individual or entity authorized to hold or administer the assets of a trust. (fiduciaire)

1.129. Tutor

In the context of civil law, a person who has been lawfully appointed to the care of the person and property of a minor. (tuteur)

1.130. Two year effectiveness review

A review, conducted every two years (at a minimum), by an internal or external auditor to test the effectiveness of your policies and procedures, risk assessment, and training program. (examen bisannuel de l'efficacité)

1.131. Valid

In respect of a document or information that is used to verify identity, appears legitimate or authentic and does not appear to have been altered or had any information redacted. The information must also be valid according to the issuer, for example if a passport is invalid because of a name change, it is not valid for FINTRAC purposes. (valide)

1.132. Verify identity

To refer to certain information or documentation, in accordance with the prescribed methods, to identify a person or entity (client). (vérifier l'identité)

1.133. Very large corporation or trust

A corporation or trust that has minimum net assets of \$75 million CAD on its last audited balance sheet. The corporation's shares or units have to be traded on a Canadian stock exchange or on a stock exchange designated under subsection 262(1) of the Income Tax Act. The corporation or trust also has to operate in a country that is a member of the Financial Action Task Force (FATF). (personne morale ou fiducie dont l'actif est très important)

1.134. Violation

A contravention of the Act or the regulations that is designated as a violation by regulations made under subsection 73.1(1). (violation)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

1.135. Virtual currency

Means:

1. (a) a digital representation of value that can be used for payment or investment purposes that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or
2. (b) a private key of a cryptographic system that enables a person or entity to have access to a digital representation of value referred to in paragraph (a).

(monnaie virtuelle)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

1.136. Virtual currency exchange transaction

An exchange, at the request of another person or entity, of virtual currency for funds, funds for virtual currency or one virtual currency for another. (opération de change en monnaie virtuelle)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.137. Virtual currency exchange transaction ticket

A record respecting a virtual currency exchange transaction—including an entry in a transaction register—that sets out:

1. (a) the date of the transaction;
2. (b) in the case of a transaction of \$1,000 or more, the name and address of the person or entity that requests the exchange, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
3. (c) the type and amount of each type of funds and each of the virtual currencies involved in the payment made and received by the person or entity that requests the exchange;
4. (d) the method by which the payment is made and received;
5. (e) the exchange rates used and their source;
6. (f) the number of every account that is affected by the transaction, the type of account and the name of each account holder;
7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
8. (h) every transaction identifier, including the sending and receiving addresses.

(fiche d'opération de change en monnaie virtuelle)

Reference:
PCMLTFR, SOR/2002-184, s. 1(2).

1.138. Working days

In respect of an electronic funds transfer (EFT) report or a large virtual currency transaction report, a working day is a day between and including Monday to Friday. It excludes Saturday, Sunday, and a public holiday. (jour ouvrable)

2. Appendix 2: Detailed Procedures for Risk Assessment development

10.3 Risk Assessment

MBs are required to conduct a risk assessment of their business by reviewing and documenting potential money laundering/terrorist financing risks. This, in turn, helps establish policies and procedures to detect and mitigate these risks and their potential/real impact.

From a fundamental perspective, “risk” is the likelihood of a negative occurrence or even happening and its outcome/consequences. From a money laundering and terrorist financing perspective, risk is at:

- The national level: Threats and vulnerabilities presented by money laundering/terrorist financing that put Canada’s financial system at risk, as well as the safety and security of Canadians. As an example, terrorist groups that operate and pose in Canada as illegal non-profit organizations fundraise and launder those funds through the financial system to fund terrorist activity locally and abroad.
- The reporting entity level: Internal and external threats and vulnerabilities that could open MBs to the possibility of being used to facilitate money laundering or terrorist financing. For example, a possible money laundering or terrorist financing risk at the reporting entity level could be conducting business with clients in high-risk or comprehensively sanctioned jurisdictions.

As part of the risk assessment, it is essential to distinguish between the inherent risk, which is the risk of an event or circumstance existing before a control/ mitigation measure is implemented, and the residual risk, which is the level of risk that remains after control/mitigation measures have been implemented.

10.4 Conducting a Risk Assessment

This is called a Risk-Based Approach (“RBA”) by conducting a risk assessment and using that information to inform policies and procedures. This approach is the approach MB is required to undertake. When assessing and documenting the money laundering and terrorist financing risk, the following must be considered:

- Clients and business relationships, including their activity patterns and geographical locations;
- Products and services and delivery channels offered;
- The geographical locations where business is conducted;
- The risk emerging from new developments or technologies that are intended to be introduced and their potential impact on clients, business relationships, products, services or delivery channels or the geographic location of business activities; and

- Any other relevant factor that could affect the business, such as employee turnover, current or changes to industry rules and regulations.

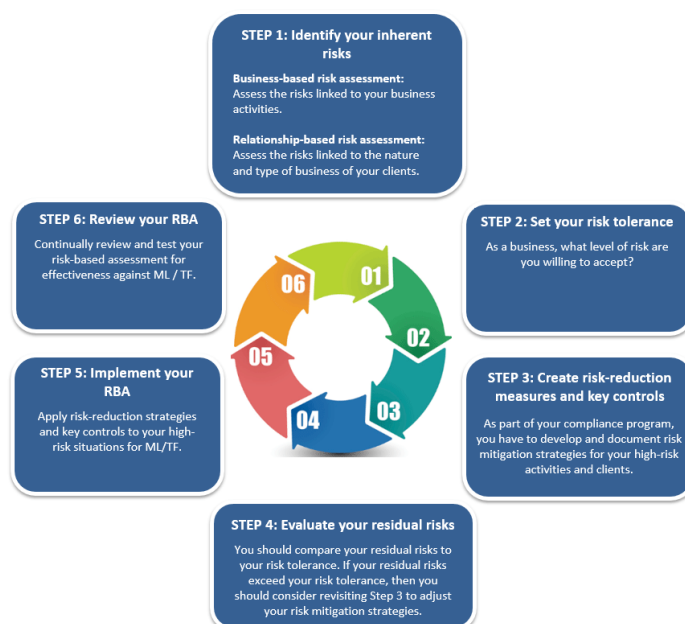
Alongside the risk assessment, it is essential to identify the risks and the controls currently in place to mitigate those risks. This is done by conducting ongoing monitoring of business relationships for the purpose of:

- Keeping client identification information and, where required, beneficial ownership and business relationship information up to date according to the client's assessed risk level
- Reassessing the level of risk associated with transactions and activities and
- Applying special measures to those transactions and business relationships identified as high-risk.

An RBA is beneficial because it helps identify gaps and weaknesses in the overall compliance program. The legislation does not prohibit high-risk activities or business relationships; however, controls are in place for these types of activities to mitigate the risks, along with the application of special measures. The assessment of risk and mitigation measures is an ongoing activity since the risk will change or evolve. At a minimum, the risk-based approach is to be reviewed and updated as part of the annual policy update.

10.5 Completing a Risk Assessment for Mortgage Brokers

Completing a risk assessment follows the risk-based approach and is done in 6 steps. Below is a diagram of the RBA cycle:



To prevent confusion, this policy divides the **business-based** and **relationship-based** risks as formatted on the FINTRAC website.

10.5.1 Step 1: Identifying Inherent Risk of Money Laundering/Terrorist Financing



The first step in conducting a risk assessment is identifying the inherent risk. This is completed by understanding the inherent risk from a business-based and relationship-based perspective.

10.5.2 Business-Based Risk Assessment

Consider the business as a whole when conducting a business-based risk assessment. Document mitigation controls for areas identified as high-risk. The number of risks identified will vary depending on the type of business activities conducted and the products and/or services offered. It is important to identify the business's inherent risks in relation to money laundering and terrorist financing. The following elements must be included as part of a business-based risk assessment.

1. A combination of products, services, and delivery channels is offered by the business.
2. Geographic locations the business operates.
3. The impact of new developments and technologies that affect operations.
4. Other relevant factors.

10.5.2.1 Products, Services, and Delivery Channels

Identify all the products, services, and delivery channels or ways in which they combine that may pose higher risks of money laundering or terrorist financing. Delivery channels are mediums through which products and/or services are offered to clients or transactions are conducted.

Please click the link for examples of [high-risk indicators and considerations for products, services and delivery channels](#).

10.5.2.2 Geography

Where the business operates or undertakes activities should be assessed from a geographic point of view about money laundering and terrorist financing. This assessment includes the immediate surroundings, rural or urban, province or territory and multiple jurisdictions within Canada or other countries.

Please click on the link to see examples of [high-risk indicators and considerations for geography](#).

10.5.2.3 New Developments and Technologies

Identify the risks associated with new developments and the adoption of new technologies within the business. Before any new technology, service, activity, or location is implemented, the potential for money laundering and terrorist financing must be assessed.

Please click on the link to see examples of [high-risk indicators and considerations for new technologies](#).

10.5.2.4 Other Relevant Factors

Identify other relevant factors that could impact the money laundering and terrorist risk.

Please click on the link to see examples of [high-risk indicators and considerations for other relevant factors](#).

Using a worksheet is an easy way to document the inherent risk related to the **business-based risk assessment**.

10.5.3 Relationship-Based Risk Assessment

Once the business-based risk assessment is completed, you must focus on the last element of the risk assessment, which consists of the MBs' clients and the business relationships MBs have with them.

As part of entering into a business relationship, keep a record of the purpose and intended nature of the business relationship. This should be reviewed periodically/according to the KYC/CDD renewal process. To conduct a relationship-based risk assessment and identify the inherent risk of money laundering and terrorist financing for the clients. Identification of money laundering and terrorist financing risk can be done for each client or grouping of clients with similar characteristics. Similar to the above, the following needs to be assessed but from a relationship perspective:

1. The combination of products, services, and delivery channels the clients use.
2. The geographic locations of the clients and their transactions.

3. The new developments and technologies available to the clients.
4. Client characteristics and the patterns of activities or transactions.

10.5.3.1 Products, Services, and Delivery Channels

The relationship-based portion of the risk assessment looks specifically at the products, services, and delivery channels clients use and the potential impact on the client's risk.

10.5.3.1.1 Product Risk

All products offered to clients must be part of the risk assessment. Products that allow for anonymity or where the source of funds is unknown are considered higher risks. For larger MB businesses, a review of the products should be completed with the product owner/employee who handles them to ensure the completeness of the risk assessment.

10.5.3.1.2 Service Risk

Services identified by a government authority or a credible source as potentially posing a high risk must be included as part of the risk assessment.

10.5.3.1.3 Delivery Channel

Delivery channels must be included in the risk assessment. Channels that allow for non-face-to-face transactions pose a higher inherent risk. These channels can be used to obscure the identity of a client or beneficial owner and, therefore, pose a higher risk. Some channels may have become part of everyday activity but should be considered in combination with other risk factors that could make a specific element, client, or group of clients high-risk.

Please click on the link to see relationship-based examples of [higher risk indicators and considerations for products, services and delivery channels](#) provided on the FINTRAC website.

10.5.3.2 Geography

In relationship-based risk assessment, the geographical location of clients and business relationships and the overall risk impact must be assessed. Money laundering and Terrorist financing risk increases when funds are received from or sent to high-risk jurisdictions and when a client has a material connection to a high-risk country. The risk should focus on the MB's clients and business relationships, which reside in high-risk jurisdictions or with transactions going to or coming from high-risk jurisdictions.

Please click on the link to view relationship-based examples of high-risk indicators and considerations for geography on the FINTRAC website.

10.5.4 Impacts of New Development and Technologies

The relationship-based risk assessment examines the potential impact that new developments and technologies could have on the MB's clients and business relationships. Properly assessed and reviewed, these developments and technologies may provide a layer of anonymity.

Please click the link to see relationship-based examples on the FINTRAC website.

10.5.5 Client Characteristics and Patterns of Activity or Transactions

When conducting the relationship-based risk assessment for client characteristics and patterns of activity or transactions, the business relationship must be reviewed, considering its purpose and intended nature of the business relationship. By examining the relationship between the client's activities and transactional patterns, a more accurate determination of a client's money laundering and terrorist financing risk can be achieved. This review is to be clearly documented in the procedures.

Certain factors increase a client's overall money laundering and terrorist financing risk and should be included in the assessment:

- The criminal history of the client regarding a designated offence;
- Unknown source of funds;
- The beneficiary of the transaction is unknown;
- The individuals conducting the transaction are unknown;
- Absence of detail in the transaction records;
- Unusual speed, volume, and frequency of transactions; or
- Unexplained complexity of accounts or transactions.

Certain factors also decrease a client's money laundering and terrorist financing risk. They include:

- A low volume of activity;
- A low aggregate balance;
- Low dollar value transactions or
- Source of funds that are subject to a regulatory scheme. (for example, a Registered Retirement Savings Plan)

Some client characteristics or activity patterns pose an inherently higher risk of ML/TF. For examples, see the below links to the FINTRAC website:

- For relationship-based examples of [higher-risk client characteristics and patterns of activity](#), see Annex 5 Table 12
- Client characteristics that can be considered higher risk, see and
- [For additional higher risk indicators and related considerations](#), see Annex 5 Table 13.

10.5.6 Scoring Relationship-Based Risk Assessment

Assessing the money laundering or terrorist financing risk can be performed on individual clients or groups of clients. When conducting a review on groups of clients, clustering those with similar characteristics is the most effective way of doing this activity. For example, grouping clients with comparable incomes, occupations, portfolios, or types of transactions is effective.

Where one high-risk indicator is identified for a client, it does not mean that the client poses a high risk, except for the three indicators in this [link](#).

Examples of higher risk indicators	Rationale
The client is in possession or control of property that the MB know/believes is owned or controlled by or on behalf of a terrorist or a terrorist group	The MB is required to send a terrorist property report to FINTRAC if the MB is in possession of property or know/believe is owned or controlled by or on behalf of a terrorist or a terrorist group. This includes information about transactions or proposed transactions relating to that property. Once the MP files a terrorist property report, the client automatically becomes high-risk.
The client is a foreign PEP	A foreign PEP is an individual who is or has been entrusted with a prominent function. Because of their position and the influence, they may hold a foreign PEP, their family members and their close associates are vulnerable to ML/TF and other offences such as corruption. As a business, the MB must consider a foreign PEP, their family members and their close associates as a high-risk client.

The entity has a complex structure that conceals the identity of beneficial owners	When the MB cannot obtain or confirm the ownership and control information of a corporation or an entity, the MB is required to verify the identity of the most senior managing officer of the entity and treat the entity as high-risk, and apply the prescribed special measures as stated in the PCMLTFRs. For more information, please consult FINTRAC's Beneficial ownership requirements guidance. It is important to note that when information is available on beneficial ownership, there may be other information or indicators that would make this relationship pose a higher risk.
--	--

The relationship-based risk assessment model combines the client's products, services, geographical risk, and characteristics and patterns of activity.

***Every high-risk client (or group of clients) must be subjected to prescribed measures. These measures should be clearly documented in the procedures and documented in terms of how they are applied to the high-risk client/group.**

Create a worksheet to document the relationship-based risk Assessment's inherent risks.

Business Relationships	Customer Risk Rating	Rationale
Identify business relationships and/or high-risk clients (individual or as groups)	Rate each business relationship and/or client (group of clients) Low, Medium or High	Explains the risk rating assigned to each business relationship and/ or client (group of clients)
Group A/Client A	Low-Risk	Receive standard transactions/payments in line with client profile
Group B/Client B	High-Risk	Receive virtual currency payments and/or large cash transaction payments from the client, which appear to beyond their means.

10.5.7 Step 2: Setting Risk Tolerance

STEP 2: Set your risk tolerance

As a business, what level of risk are you willing to accept?

Risk tolerance should be determined by considering the following types of risk that affect the organization.

- Regulatory risk;
- Reputational risk;
- Operational risk;
- Legal risk; or
- Financial risk.

The PCMLTFA and associated Regulations state that reporting entities have obligations when they identify high-risk business activities and high-risk clients. Setting a high-risk tolerance does not allow reporting entities to avoid these obligations.

10.5.8 Step 3 Creating Risk Reduction Measures and Key Controls

STEP 3: Create risk-reduction measures and key controls

As part of your compliance program, you have to develop and document risk mitigation strategies for your high-risk activities and clients.

After identifying the risks related to money laundering and terrorist financing for the business, it is essential to implement risk mitigation measures, including the implementation of controls to address those risks that have been identified. It includes:

- 1) In all situations, the business must implement internal controls that mitigate the overall risk.
- 2) For the business-based risk assessment, all the high-risk elements identified must have clearly documented mitigating controls/measures.
- 3) For client and business relationships, ensure
 - a. Ongoing monitoring is conducted for all business relationships

- b. A record must be kept of all measures and information obtained through the monitoring
- 4) For high-risk clients and business relationships, all prescribed special measures must be adopted, including:
 - a. Conducting enhanced monitoring of clients and business relationships
 - b. Taking enhanced measures to verify identity and keep client information up to date.

The implementation of risk mitigation measures allows the business to stay within its risk tolerance. The higher the risk tolerance, the more likely the business will accept higher-risk situations/clients. Where higher-risk situations/clients are accepted, stronger mitigation measures/ controls should be in place and commensurate with the level of risk, and the residual risk must be reasonable and acceptable.

10.5.9 Step 4: Evaluating the Residual Risk

STEP 4: Evaluate your residual risks

You should compare your residual risks to your risk tolerance. If your residual risks exceed your risk tolerance, then you should consider revisiting Step 3 to adjust your risk mitigation strategies.

The residual risk and risk tolerance should align. No matter how robust the mitigation measures are, there will always be exposure to residual money laundering and terrorist financing risk. If, after creating the risk mitigation measures, the residual risk is greater than the entity's risk tolerance, it means that the measures and controls do not mitigate high-risk situations or high-risk clients. Go back to Step 3 and review the mitigation measures that were put in place.

There are two types of residual risk:

Tolerated risk: Risks that are accepted because there is no benefit in reducing them. Tolerated risks may increase over time. For example, when a new product is introduced or a new threat appears,

Mitigated risk: Risks that have been reduced but not eliminated. In practice, the controls in place may fail from time to time (a large virtual currency transaction is not reported due to a failure in the transaction review process).

Below is an example of an MB further mitigating risk because, over time, their risks and clients have evolved.

Illustrative Example – Not AKAL-Specific:

Mortgage Broker ABC Corp (MB “ABC Corp”) offered and arranged mortgages for only

the larger lenders such as Canadian banks and Credit Unions in Canada. ABC Corp lending partnerships prohibited relationships with nontraditional lending entities inside and outside Canada. ABC Corp also restricted their brokerage services to Canadian residents only. The policy and risk assessment only ever focused on these types of business and customer relationships; however, as the Canadian real estate market has proven to be fairly stable with a high rate of return, international investors and large fintech have been seeking services from ABC Corp.

Conclusion: ABC Corp now feels that the current mitigation measures are no longer sufficient to meet the entities' (yet realized) increasing risk tolerance. Therefore, the residual risk from the previously established mitigation measures has increased and exceeds the current risk tolerance.

ABC Corp will add new mitigation measures to realign the residual risk with its new risk tolerance level. Examples of new additional mitigation measures include:

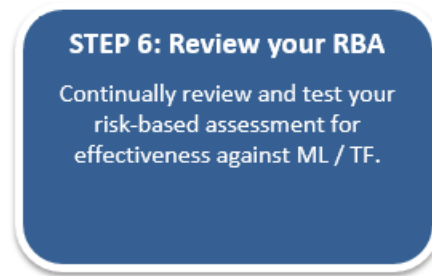
- Prohibition on the onboarding of clients residing outside of Canada in high-risk jurisdictions
- Clients residing outside of Canada (in a non-high-risk jurisdiction) must have employment, and the transactional activity must align with their verified source of wealth and funds.
- Internal approval must be obtained for all non-residents.
- Lending partnership arrangements with Fintech only trading on a Canadian or US stock exchange and must have a balance sheet of over CAD 500 million.
- All Fintechs must be incorporated in Canada or the US and have an operating location in Canada.

10.5.10 Step 5: Implementation of the Risk-based Approach



The risk-based approach must be implemented as part of day-to-day activities. The risk assessment must be well documented and detailed as part of the compliance program. Risk and risk mitigation requires the leadership and engagement of senior management. Senior management or the business owner is ultimately accountable and is responsible for making decisions related to policies, procedures and processes that mitigate and control money laundering and terrorist financing risk.

10.5.11 Step 6: Review the RBA



The program's effectiveness is tested as part of the periodic review (to be conducted a minimum every two years). That includes a review of the following:

- Policies and procedures
- Risk assessment related to money laundering and terrorist financing
- Training program

As the business model evolves or changes and new products or services are offered, the Mortgage Broker must update the risk assessment. When testing the effectiveness of the risk assessment, all components must be covered, including:

- The policies and procedures on the risk assessment
- The risk mitigation strategies and
- Special measures include enhanced monitoring procedures.

The overall expectations of FINTRAC expectations are summarized in the “Annex 1- FINTRAC RBA Expectations” section. Click the [link](#) and review the summary of the information.

3. Appendix 3: Training

10.6 Training topics/ materials and methods for delivery

The training plan includes topics covered in the training program and the source of the training materials that cover these topics.

The training plan includes information on how the training is delivered. Methods include self-directed learning, information sessions, face-to-face meetings, classroom conferences and on-the-job training. Instruction will be provided in-house and, where needed, through external service providers. If training is done in-house, it will be conducted by dedicated staff. All external service providers' content will be reviewed and assessed for suitability. All instructors, whether internal or external, know the PCMLTFA and its associated Regulations.

10.7 Training Frequency

The frequency of the ongoing training program is described in the training plan. Training is expected to be delivered at regular intervals (monthly, semi-annually or annually). When an employee is onboarded, there is a role change or after a procedure/policy change. A record of the training must be kept. It includes what training topic has been delivered, the training date, and a list of the attendees. The purpose of the training record is to help keep track of when the next scheduled training needs to be delivered and to demonstrate that the training program is being offered on an ongoing basis.

If, as an MB, there are no employees, brokers or individuals authorized to act on the MB's behalf, the MB is not required to have a training program or plan.

4. Appendix 4: STRs

10.7.1 How to submit a STR to FINTRAC

The preferred method of submitting a STR to FINTRAC is electronically using the following options:

- [FINTRAC Web Reporting System](#) (FWR) (geared towards reporting entities with lower reporting volumes);
- [FINTRAC API report submission](#) (secure system-to-system transfer of report information).

Paper forms are permitted in the above cases; see the link. A copy of the submitted report must be kept for at least five years after the day it is sent.

10.7.2 Changes to STR

A STR may be amended; however, a correction for the change must be explained. If a subsequent change needs to be made to an already submitted report, the change must be made, and the revised report must be submitted to FINTRAC within 20 days of the date the request was made for the change.

10.7.3 Compliance Program and STRs

Please review the procedures to determine how to identify and assess suspicious transactions and the submission process for STRs to FINTRAC. For further information on the form and structure of the STR, see the [link](#).

As part of the two-year effectiveness review, the detecting, assessing, and submission of STRs must be reviewed. The effectiveness review plan documents the approach taken in the effectiveness review. It should be noted that anywhere where a suspicious transaction/activity is conducted in tandem involving a disbursement involving a large cash transaction or a large virtual currency transaction, the respective report disbursement type is filed in addition to the STR. Where there are instances where a STR needs to be filed in addition to a terrorist property report, please see the policy section on **Reporting Terrorist Property** in conjunction with the procedures. A copy of the submitted STR to FINTRAC must be kept for at least five years after the day the report is sent.

Reasonable measures must be taken to verify the identity of every person or entity conducting or attempting a suspicious transaction. This means it is expected that the MB ask questions to verify the person/entity's identity unless it is believed that in doing so, they will be tipped off. Reasonable measures regarding third-party determination

are also required. This is where a determination is made as to whether a person or entity is acting on behalf of a third party. Third-party determination is a reasonable measure unless, in asking questions, it is believed that the client will be tipped off.

Ministerial directives requirements must be considered alongside STR reporting requirements. The ministerial directives are directives issued under the PCMLTFA which require MBs to apply countermeasures to transactions coming from and or going to designated foreign jurisdictions or entities and recommend the introduction of regulations restricting reporting entities from entering into a financial transaction coming from or going to designated foreign jurisdiction or entities. See the [link](#) for more information.

Where there are instances of non-compliance related to STR reporting, a voluntary self-declaration of non-compliance must be reported to FINTRAC. See the [link](#) for more details.

10.7.4 Reporting Subsequent Suspicious Transactions

Subsequent transactions after the initial STR report must continue to be reported provided the suspicion remains. The client must be reassessed to verify that the level of suspicion has not changed and that it is part of the risk assessment and ongoing monitoring. If there is continued STR reporting in relation to a particular person or entity, reference the previous STR report by including:

- The reporting entity report reference number and the reporting entity transaction reference number;
- The reasonable grounds to suspect (facts, context and money laundering and terrorist financing indicators) that were included in the first STR submission;
- Any new additional information.

Suppose the basis of the STR is due to new facts, context, money laundering, or terrorist activity financing indicators revealed during the assessment of the client. In that case, this new information must be included in the STR. The information provided in the STR report must be complete and accurate. It is important to submit a high-quality report. For FINTRAC expectations for completing a STR, as well as the Common STR Reporting Deficiencies and Instructions on how to complete the report, see the [link](#).

5. Appendix 5: Listed Person or Entity Property Reports (LPEPRs)

10.7.5 Submission of LPEPRs

A Listed Person or Entity Property Report must be submitted to FINTRAC immediately when the Brokerage is required to make a disclosure under section 83.1 of the Criminal Code, an order or regulation made under the United Nations Act, an order or regulation made under the Special Economic Measures Act, or subsection 7(2) of the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law). The LPEPR replaces the former Terrorist Property Report and covers terrorist and sanctioned property.

10.7.6 The LPEPR form is available from FINTRAC's paper reporting forms page. The report must be submitted by fax where the Brokerage has the technical capability to do so:

1-866-226-2346

If fax submission is not technically possible, submit the LPEPR by regular or registered mail to:

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

There is no official acknowledgment of receipt after an LPEPR is submitted to FINTRAC. A copy of every submitted LPEPR must be retained for at least five years from the day the report is sent and may be retained electronically if a paper copy can be readily produced.

10.7.7 Other Activities Associated with LPEPRs

STRs must be submitted if a transaction was attempted or completed and involves property that is **known** to be owned or controlled by or on behalf of a terrorist group or that is **believed** to be owned or controlled by or on behalf of a listed person (for which a LPEPR submission is required), **also submit an STR** to FINTRAC. This is because the threshold of **reasonable grounds to suspect** that the transaction or attempted transaction is related to the commission or attempted commission of a terrorist activity financing offence has been met.

Reasonable grounds to suspect means there is a [possibility](#) that an ML or TF offence has occurred based on an assessment of facts, context, and indicators, and one

can present the reasons why it is suspicious without proof or verification.

Having **reasonable grounds to believe** is a higher threshold and means there is a [probability](#) that an ML or TF offence has occurred. They can present a set of verified facts that can be proven and support this belief.

If one does not know or believe that the property in possession or control is owned or controlled by or on behalf of a terrorist group or listed person, the requirement to disclose to the RCMP or CSIS is not triggered, and therefore, a LPEPR is not required. However, suppose it is suspected that the property in possession or control is owned or controlled by or on behalf of a terrorist group or listed person. In that case, an STR must be submitted to FINTRAC if an attempted or completed transaction was associated with this property.

Refer to the procedures for further information on the LPEPR submission process, including the following:

- The process of identifying terrorist property or sanctioned property;
- The quality control process to ensure LPEPRs are entirely accurate and submitted immediately.

Listed person or entity property reporting is included in the training program and plan. A copy of each LPEPR submitted to FINTRAC must be retained for at least five years from the day the report was sent. A copy of the report can be kept in electronic format, provided a paper copy can be produced from it.

10.7.8 Property and Listed Person or Entity Scope

Property includes anything owned or controlled by a person or entity, whether tangible or intangible, including cash, monetary instruments, virtual currency, accounts, securities, jewellery and precious metals or stones, real estate, insurance policies and physical goods such as equipment, vehicles or artwork. A transaction or attempted transaction does not need to occur for an LPEPR obligation to arise.

A listed person or entity includes, as applicable, a terrorist group under the Criminal Code; a person or entity subject to an order or regulation under the United Nations Act or Special Economic Measures Act; a foreign state subject to an applicable order or regulation; or a person subject to an order or regulation under section 4 of the Sergei Magnitsky Law.

When to Also Consider an STR

If a transaction was attempted or completed involving property owned or controlled by or on behalf of a listed person or entity, the Brokerage must submit the required LPEPR

and separately assess whether the facts, context and indicators create reasonable grounds to suspect that the transaction is related to money laundering, terrorist activity financing or sanctions evasion. If the STR threshold is met, an STR must also be submitted to FINTRAC.

- If the applicable disclosure threshold for an LPEPR is not met but the Brokerage suspects that property may be owned or controlled by or on behalf of a listed person or entity, the Brokerage must assess whether an STR is required for any associated attempted or completed transaction.
- Compliance Program and Quality Control

The Procedures must document the process for identifying terrorist and sanctioned property; screening and escalation to the Compliance Officer; making any required external disclosure; completing, quality-controlling and submitting LPEPRs immediately; retaining reports for five years; considering related STR obligations; incorporating LPEPR risk indicators into the risk assessment; training affected personnel; and testing LPEPR controls as part of the two-year effectiveness review.

6. Appendix 6: LCTR

10.8 Large Cash Transaction Report (“LCTR”)

MBs are responsible for submitting a large cash transaction report when in receipt of \$10,000 CAD or more in cash (or a foreign equivalent) during a single transaction. This includes:

- Transactions that fall under the 24-hour rule;
- Transactions that the MB have authorized another person or entity to receive on their behalf.

Cash includes:

- Coins and banknotes issued by the Bank of Canada that are intended for circulation in Canada;
- Coins and banknotes of countries other than Canada;
- [Fiat currency](#).

Cash does **not** include:

- Other forms of [funds](#) such as cheques, money orders or other similar negotiable instruments;
- [Virtual currency](#).

A service provider can also submit a Large Cash Transaction Report on behalf of the MB. Where an MB has engaged a service provider to submit a form on their behalf, the MB is ultimately responsible for meeting the requirements under the PCMLTFA and its Regulations. The legal responsibility cannot be delegated. Where a service provider is obtained to submit reports on behalf of the entity, all arrangements are entered via a written agreement. For further information on the FINTRAC website regarding service provider arrangements, please click on the [link](#).

An LCTR must be submitted within 15 calendar days after the day on which the MB received the cash.

10.8.1 24-hour rule

A Large Cash Transaction Report to FINTRAC must also be submitted in accordance with the 24-hour rule. That occurs when:

- **Two or more** amounts in cash that total CAD 10,000 or more (or a foreign equivalent) within a consecutive 24-hour window are received, **and**

- It is **known** that the transactions are:
 - Conducted by the same person or entity;
 - Conducted on behalf of the same person or entity ([third party](#)) **or**
 - For the same [beneficiary](#).

Please see here for further information on the 24-hour rule. A copy of the submitted report must be kept for at least five years from the day it was created.

10.8.2 Foreign Currency

If the MB receives cash in a foreign currency, convert it into Canadian dollars using the exchange rate published by the Bank of Canada at the time of the transaction (see link here). This determines whether the reporting threshold of CAD 10,000 is met. If an exchange rate is not published by the Bank of Canada, the rate given by the business at the time of the transaction should be used to determine reportability.

10.8.3 Reporting Large Cash Transactions

The preferred method of submitting a large cash transaction report to FINTRAC is electronically using the following options:

[FINTRAC Web Reporting System](#) (FWR) (geared towards reporting entities with lower reporting volumes)

[FINTRAC API report submission](#) (secure system-to-system transfer of report information)

Paper forms are permitted in the above cases; see the [link](#).

Please see the link for more details on how to fill out an LCTR, as well as the form and structure of the report.

Review the procedures to understand how to:

- Select exchange rates and their source;
- Aggregate transactions;
- Determine if the client is a person or an entity;
- Submit reports to FINTRAC.

10.9 Verifying the Identity of Persons and Entities

There are requirements on when and how to verify the identity of persons and entities for large cash transactions. Please consult the section on Know Your Client and the procedures for additional information.

For additional information, consult the following verification methods from FINTRAC:

- [Methods to verify the identity of persons and entities;](#)
- Consult the policy and procedures in conjunction with guidance from FINTRAC on when to verify the identity of persons and entities.

10.10 Third-Party Determination

Third-party determination must be conducted when reporting large cash transactions or keeping a large cash transaction record. A third party is a person or entity that instructs another person or entity to conduct a transaction or activity on their behalf. As such, the third party is the instructing party to the transaction or activity and is also understood as the "on behalf of" party. Please consult the section on Know Your Client and the procedures for additional information.

For additional information, consult the following information on third-party determination requirements from FINTRAC:

[Third-party determination requirements](#)

10.11 Ministerial Directive

Ministerial directives requirements must be considered alongside large cash transaction reporting requirements.

For additional information, consult the following information on ministerial directive requirements from FINTRAC:

[Ministerial directives and transaction restrictions](#)

10.12 Voluntary Self-Declaration of Non-Compliance

Where there are instances of non-compliance related to large cash transaction reporting, a voluntary self-declaration of non-compliance must be reported to FINTRAC. See the [link](#) for more details.

10.12.1 LCTRs and STRs

In addition to reporting and LCTR, there may be a requirement to submit an STR to FINTRAC, provided the reasonable grounds threshold has been met. Therefore, if that threshold is met, both reports must be submitted. Please see the section in the policy on STR reporting for more details.

10.12.2 Exceptions to Reporting Large Cash Transactions

If an amount is received of \$10,000 or more in cash in a single transaction from the following entities, an LCTR report is not required to be submitted:

- A [financial entity](#);
- A [public body](#), or
- A person who is acting on behalf of a client that is a financial entity or public body.

10.13 AKAL APPLICABILITY NOTE:

NOT APPLICABLE UNDER THE CURRENT BUSINESS MODEL. AKAL Mortgages does not accept cash from clients. This section is retained for regulatory reference and must be reassessed before any change in business practice that permits acceptance of cash.

7. Appendix 7: LVCTR

10.13.1 Submitting Large Virtual Currency Transaction Report (“LVCTR”)

MBs are responsible for submitting a large virtual currency transaction report when in receipt of \$10,000 CAD or more during a single transaction. This includes:

- Transactions that fall under the 24-hour rule;
- Transactions that the MB have authorized another person or entity to receive on their behalf.

Virtual currency is a digital representation of value or the private key of a cryptographic system that enables access to a digital representation of value that can be used for payment or investment purposes.

Virtual currency **is not** a fiat currency, but it can be readily exchanged for:

- Funds; or
- Another virtual currency that can be exchanged for funds.

For greater clarity, this definition does not include certain digital currencies, such as:

1. Those that can only be used within a self-contained virtual environment or
2. A digital currency that can be redeemed for goods and services but not easily converted into funds.

For example, such digital currencies include:

- Those used for online gaming, which are not exchangeable for funds or virtual currencies, or
- Those that can only be redeemed for gift cards and loyalty programs

10.13.2 24-hour rule

A Large Virtual Currency Transaction Report needs to be submitted to FINTRAC in accordance with the 24-hour rule. This occurs when:

- **Two or more** amounts of virtual currency that total CAD 10,000 or more within a consecutive 24-hour window are received, **and**
- It is **known** that the transactions are:
 - Conducted by the same person or entity;
 - Conducted on behalf of the same person or entity ([third party](#)) **or**

- For the same [beneficiary](#).

For further information on the 24-hour rule, please see [here](#).

To determine if a transaction is reportable, one must receive the transaction, where it cannot be reversed or cancelled, and the LVCTR must be submitted within five working days after the day on which the transaction was received.

10.13.3 Exchange Rate

Since the Bank of Canada does not publish an exchange rate for virtual currency, the rate given by the business at the time of the transaction should be used to determine reportability.

The process for establishing the exchange rate is outlined in the procedures.

10.13.4 Large Virtual Currency Transaction Reporting

The preferred method of submitting an LVCTR to FINTRAC is electronically using the following options:

[FINTRAC Web Reporting System](#) (FWR) (geared towards reporting entities with lower reporting volumes)

[FINTRAC API report submission](#) (secure system-to-system transfer of report information)

Paper forms are permitted if the MB lacks the technical capabilities; see the link. A copy of the submitted report must be kept for at least five years from its creation date.

Please see the link for further information on completing an LVCTR and on the report's form and structure.

Review the procedures to understand how to:

- Select exchange rates and their source;
- Aggregate transactions;
- Determine if the client is a person or an entity;
- Submit reports to FINTRAC.

10.14 Verifying the Identity of Persons and Entities

There are requirements on when and how to verify the identity of persons and entities for large virtual currency transactions. Please consult the section on Know Your Client and the procedures for additional information.

For additional information, consult the following verification methods from FINTRAC:

[Methods to verify the identity of persons and entities](#)

Consult the policy and procedures in conjunction with guidance from FINTRAC on when to verify the identity of persons and entities.

[All FINTRAC guidance – Know your client's requirements](#)

10.14.1 Third-Party Determination

Third-party determination must be conducted when reporting on large virtual current transactions or when keeping a large virtual currency transaction record. A third party is a person or entity that instructs another person or entity to conduct a transaction or activity on their behalf. As such, the third party is the instructing party to the transaction or activity and is also understood as the "on behalf of" party. Please consult the section on Know Your Client and the procedures for additional information.

For additional information, consult the following information on third-party determination requirements from FINTRAC:

[Third-party determination requirements](#)

10.14.2 Ministerial Directive

Ministerial directives requirements must be considered alongside large virtual currency transaction reporting requirements.

For additional information, consult the following information on ministerial directive requirements from FINTRAC:

[Ministerial directives and transaction restrictions](#)

10.14.3 Voluntary Self-Declaration of Non-Compliance

Where there are instances of non-compliance related to large virtual currency transaction reporting, a voluntary self-declaration of non-compliance needs to be reported to FINTRAC. See the [link](#) for more details.

10.14.4 Exceptions to Reporting Large Virtual Currency Transactions

A large Virtual Currency Transaction Report is not required where in receipt of:

- Two or more amounts in virtual currency that are each individually equivalent to less than \$10,000, but together total \$10,000 or more within 24 consecutive hours, when the amounts are for a beneficiary that is:
 - A [public body](#);
 - A very large corporation or trust; or

- An administration of a pension fund that is regulated under federal or provincial legislation.
- Virtual currency in an amount equivalent to \$10,000 or more in a single transaction if the virtual currency is received as:
 - Compensation for the validation of a transaction that is recorded in a [distributed ledger](#) or
 - A nominal amount of virtual currency for the sole purpose of validating another transaction or a transfer of information.
- Virtual currency for the MBs' own operational purposes.

For example, the receipt of virtual currency when it is received or purchased as holdings for the business does not need to be reported.

10.15 AKAL APPLICABILITY NOTE:

NOT APPLICABLE UNDER THE CURRENT BUSINESS MODEL. AKAL

Mortgages does not accept virtual currency from clients. This section is retained for regulatory reference and must be reassessed before any change in business practice that permits acceptance of virtual currency.

8. Appendix 8: Dual-process method

10.15.1 How to use a credit file under the dual-process method

A Canadian credit file can be used as one of the two pieces of information required to verify a person's identity under the dual-process method. It covers Verification Methods A, BC and C. Specifically, it can be used to confirm the person's name and address, name and date of birth, or to confirm the person's name and confirm that the person has a credit card account or a loan account. If the MB uses a credit file, it can only be used as one of the information pieces for the dual-process method; it must have existed for at least six months.

Information from a second source, for example, a property tax assessment, might be used to confirm the second category of information. In this instance, the two reliable sources are the Canadian credit bureau, which provided the credit file information, and the municipal government, which issued the property tax assessment. The information from these two sources must match the information the person provides.

If a Canadian credit bureau is used as a source, it is essentially an aggregator of information from different reliable sources. In this instance, the Canadian credit bureau must provide information from two independent tradelines, where each tradeline confirms one of the two categories of information required to verify a person under the dual process method. In this instance, each tradeline is a distinct source, not the credit bureau.

10.15.2 Record-keeping requirements for the dual-process method

The following are the record-keeping requirements when verifying a person's identity under the dual-process method:

- The person's name;
- The date the information was verified;
- The name of the two different reliable sources that were used to verify the identity of the person;
- The type of information referred to (for example, a utility statement, a bank statement, a marriage license) and
- The number associated with the information (for example, account number or, if there is no account number, a number that is associated with the information, which could be a reference number or certificate number, etc.). Suppose information was aggregated by a Canadian credit bureau and received information from two distinct sources (tradelines). In that case, the recorded

information must include the account number associated with each tradeline and not the aggregator (credit bureau) number.

The procedures describe the process that must be followed when using the dual-process method to verify a person's identity and the approach taken to ensure the information is valid and current.