Anti-Money Laundering Compliance Policy

WORLDSEC PAYMENTS LIMITED
November 2023

Contents

Preamble

This Anti Money Laundering Compliance Policy of **WORLDSEC PAYMENTS LIMITED** (the "**Company**" or "**we**") governs the Company's principles and standards to prevent money laundering, to combat terrorism, and financial crime. **WORLDSEC PAYMENTS LIMITED.** fulfills legal obligations as required by the Canadian Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and other applicable rules and regulations connected to anti-money laundering and counter-terrorist financing ("**AML/CTF**") obligations.

This AML Policy explains the current principles of anti-money laundering and counter-terrorist financing obligations and provides answers and explanations on PCMLTFA's explanation of transaction types, reporting requirements, client information and record keeping.

As a money service business in Canada, the Company ensures it is fully compliant with Canadian legislation to combat money laundering and terrorism. The Company respects and adheres to the international, foreign, and domestic laws applicable to its business.

As such, this Policy sets the terms and conditions, as well as a procedure on how we identify and verify clients, assess relevant risks, and, if necessary, report to relevant governmental authorities.

We have other internal policies on this subject matter.

Our expectations towards our employees and business partners

All employees, whether temporary, fixed-term, or permanent, and management of the Company, must comply with the Company's AML Policy, regardless of their position and location. This AML Policy also applies to all third parties, whether contractors, seconded staff, trainees, acting under the contractual responsibility of the Company.

This AML Policy is equally binding for all employees and contracted third parties.

Our senior management is responsible for ensuring that this Policy is fully applied and communicated to our team members and third parties engaged by the Company.

We do not tolerate any illegal activities and expect our business partners to meet the same principles we demand from ourselves.

The Company Business

The Company is an authorized electronic money institution in Canada. It offers to businesses the following financial solutions:

- Foreign exchange dealing
- Money transferring
- Dealing in virtual currencies

Geography of our Services

The geography of our services encompasses the following geographical regions: Canada, USA, Venezuela, Algeria, India, Turkey, Brazil, Bangladesh and others.

Changes

This Policy and other guidance to be reviewed at least once every two years to meet the highest standards and comply with local, regional, and international regulatory requirements. This may lead to our obligations related to KYC and KYB procedures.

1. Information related to money laundering

1.1 What is money laundering?

The term "money laundering" evolved to illustrate illegal and criminal activities when individual attempts to hide the original source of money or assets gained from various illicit activities, such as bribery, tax evasion, fraud.

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC of Canada), which is the Canadian financial intelligence unit, has introduced robust anti-money laundering and anti-terrorist financing legislation and regulations attributable to financial institutions operating in Canada. FINTRAC issues various guidance that allows to learn more on money laundering.

FINTRAC of Canada recognizes three stages in the money laundering process[1], which are:

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

Going through these stages, it is possible to hide a source of income origin, and therefore, clean "dirty money." Some criminals use proceeds for various illegal purposes, such as terrorist financing, making illegal transactions. As a result, such funds come to the financial system of Canada and other countries.

1.2 Methods of Money Laundering

Criminals utilize various methods to clean money. Traditionally, these methods are use of nominees and complex transactions to hide actual ownership, smurfing, asset purchases with bulk cash, currency smuggling, gambling in casinos, virtual currencies transfers, etc.

1.3 Importance of combating money laundering

Money laundering is a multi-million dollar illegal business that brings inequality and damages to the social and economic system. Canadian authorities, together with other governments, use joint forces to deprive criminals of the profits. In recent decades, criminals have been using international and complex schemes to hide profits. Joint cooperation enables to fight against money laundering and terrorism effectively.

Canada is an active member of international organizations and cooperation with other countries to combat illegal activities.

[1] https://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng

It is a requirement of all financial institutions and certain organizations to comply with anti-money laundering legislation and adopt rules that meet Canadian and international requirements.

1.4 International Cooperation to Fight against Money Laundering

For the past decades, international cooperation between countries has been expanded, facilitating international cooperation at different levels, including governmental and business collaboration.

There have been various international initiatives that aim to detect and prosecute money laundering. Such global initiatives where Canada takes part are:

- Financial Action Task Force (FATF), more information about FATF at http://www.fatf-gafi.org;
- Egmont Group of Financial Intelligence Units (FIUs) at https://egmontgroup.org/;
- European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, more information at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=141;
- Asia Pacific Group on Money Laundering (APG), more information at http://www.apgml.org;
- Caribbean Financial Action Task Force on Money Laundering (CFATF), more information at https://www.cfatf-gafic.org;
- United Nations Single Convention on Narcotic Drugs, more information at https://www.unodc.org/pdf/convention_1961_en.pdf;
- United Nations Convention on Psychotropic Substances, more information at https://www.unodc.org/pdf/convention_1971_en.pdf;
- United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, more information at https://www.unodc.org/pdf/convention_1988_en.pdf;
- United Nations Convention Against Transnational Organized Crime, more information at https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.

It is a requirement of member countries to accept and implement the rules and principles to their local laws and regulations that are consistent with, and as comprehensive as agreed rules and principles.

Canada has enacted the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* in order to facilitate the identification of entities that conduct illegal financial transaction and to effectively fight against money laundering.

Being supportive with other international initiatives on combating money laundering, our Company has implemented internal and external policies outlining the basic framework for anti-money laundering and terrorist financing. Further, our company constantly monitors legislative developments that address this issue and adheres to Canadian legislation and international treaties implementing the best practices to combat money laundering.

1.5 A General Overview of Canadian Legislation to Combat Money Laundering

Money laundering has been legally recognized as a criminal offense in Canada under the Criminal Code within the previous decades.

Another important law is the Proceeds of Crime (Money Laundering) Act which was enacted in 2000. In 2001, the first reporting requirement came into effect for suspicious transactions. These measures were subsequently enhanced, and additional components were introduced. That same year, the scope of the Proceeds of Crime (Money Laundering) Act was expanded to include terrorist financing. This resulted in the former Proceeds of Crime (Money Laundering) Act becoming the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

Over the course of 2002 and 2003, other requirements under the PCMLTFA and related Regulations were phased-in, such as record keeping, client identification, and other reporting obligations.

In 2006, amendments to the PCMLTFA introduced changes such as the establishment of a money services businesses registry, the authority to levy administrative monetary penalties and the addition of new reporting sectors, among others. They also included measures to strengthen reporting, record keeping, client identification, and compliance regime requirements. These changes were phased in over the course of 2007 to 2009.

Substantial regulatory amendments came into play on June 1, 2021, changing or creating new obligations for reporting entities that are subject to the PCMLTFA. Aiming to prevent unauthorized transactions, the amendments include new virtual currency obligations for all reporting entities and new definitions under the PCMLTFA. They also include record keeping and reporting changes for all reporting entities, and obligations for foreign money services businesses. The amendments introduce new requirements for all reporting entities to take reasonable measures to confirm the accuracy of information regarding beneficial ownership.

The Company and anyone acting on behalf of the Company must comply with the applicable local laws.

1.6 When are we obliged to report to FINTRAC?

The Company takes any violation seriously and is committed to efficiently and timely investigate, and, if necessary, report the FINTRAC about certain transactions and property in accordance with the Canadian laws.

We ensure that our Compliance Officer, top management, and internal system is able to track and monitor violations.

In accordance with Canadian laws, we are obliged to take specific steps and report immediately to FINTRAC.

FINTRAC is an independent government agency in Canada. It operates at arm’s length from law enforcement agencies and collects, analyzes, and discloses information to help detect, prevent and deter money laundering and the financing of terrorist activities in Canada and abroad. Companies and other entities in Canada are obliged to report to FINTRAC on suspicion of money laundering and terrorist financing. Further, it analyzes information and implements other necessary actions.

The Company will immediately submit a report to FINTRAC in case of the following:

1.7 Suspicious transactions

The Company will report on any completed or attempted transaction if there are reasonable grounds to suspect that such transaction is related to the commission or attempted commission of a money laundering offense or a terrorist activity financing offense. We will report to FINTRAC or, if necessary, directly to law enforcement.

FINTRAC provides detailed information about reporting suspicious transactions to FINTRAC to which we adhere to: https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide3/str-eng.

There are different grounds and examples which would lead to our reporting obligations of suspicious transactions.

Several examples of an individual acting suspiciously:

- asks several questions about Company's reporting obligations to FINTRAC;
- wants to know how they can avoid their transaction being reported to FINTRAC;
- structures their amounts to avoid client identification or reporting thresholds;
- keeps changing their explanation for conducting a transaction or knows few details about its purpose;
- refuses or tries to avoid providing information required, or provides information that is misleading, vague, or difficult to verify;
- provides false, altered or inaccurate documentation;
- has accounts with several financial institutions in one area for no apparent reason;
- repeatedly uses an address but frequently changes the name involved;
- provides confusing details about the transaction;
- is involved in unusual activity for that individual or business;
- refuses to provide ID;
- frequently travels to a high-risk country.

Transactions constantly being made by a third party on behalf of another individual or entity:

- a client conducts a transaction while accompanied, overseen, or directed by another party
- payments to or from unrelated parties (foreign or domestic)
- client appears to be or states that they are acting on behalf of another party

Transactions to a business account with the following additional elements:

- deposits to the account are made by numerous parties that are not signing authorities or employees;
- the account activity involves wire transfers in and out of the country, which do not fit the expected pattern for that business.

Transactions frequently being made by a third party on behalf of another individual or entity:

- multiple payments made to an account by non-account holders;
- account is linked to seemingly unconnected parties.

1.8 Large cash transactions

While the Company doesn't intend to conduct any cash transactions , the Company will report to FINTRAC any transaction exceeding CAD 10,000 or more in cash in the course of a single transaction, or any transaction with two or more cash amounts of less than CAD 10,000 that total CAD 10,000 or more should such transactions occur in the future

In addition, the Company will keep the virtual currency transaction record for amounts received in virtual currency of CAD 10,000 or more in a single transaction, or across multiple virtual currency transaction that total CAD 10,000 or more within a span of 24 hours.

1.9 Terrorist property

The Company reports to FINTRAC if the Company receives property in the possession or control that we know is owned or controlled by or on behalf of a terrorist group within the meaning of the Canadian Criminal Code. Further, we will report to FINTRAC if we have property in our possession or control that we believe is owned or controlled by or on behalf of a person listed under the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism.

1.10 Electronic Funds Transfer

We are obliged to report to FINTRAC on incoming and outgoing international electronic funds transfers of CAD 10,000 or more. These can be instructions sent electronically outside Canada or from outside Canada in a single or two/more transfers.

1.11 Large Virtual Currency Transactions

The Company doesn't intend any transactions in virtual currency. 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. It is not a fiat currency, but it can be readily exchanged for funds or another virtual currency that can be exchanged for funds.

However, should such transactions occur in the future, we are obliged to report a Large Virtual Currency Transaction Report (LVCTR) to FINTRAC in the following events:

- if we receive virtual currency (VC) in an amount equivalent to CAD 10,000 or more in the course of a single transaction; or
- if we receive two or more amounts of VC, that total the equivalent of CAD 10,000 or more within a consecutive 24-hour window, by or on behalf of the same person or entity, or for the same beneficiary.

The Company must send an LVCTR to FINTRAC within five working days after the day you received the amount.

We do not have to submit an LVCTR to FINTRAC if the amount of VC is received as compensation for the validation of a transaction that is recorded in a distributed ledger, or is a nominal amount of VC received for the sole purpose of validating another transaction or transfer of information.

1.12 What are other additional measures that we implement to comply with PCMLTFA?

The Company has implemented appropriate systems that internally control and prevent money laundering or terrorist financing activities. Our internal system monitors and identifies suspicious transactions or unusual customer behavior in accordance with FINTRAC guidance. The basis of the internal control process includes:

- well-defined authorisations,
- a segregation of duties,
- client identification,
- on-going due diligence,
- reporting suspicious transactions and activities.

1.13 Internal Control System

In order to ensure the effective work of our internal control system, the Company ensures our management and team are fully aware about our AML compliance policy.

The Company is required to keep certain records after conducting specified transactions. This includes specific requirements about identifying individuals with whom a reporting entity conducts a transaction. We follow FINTRAC guidance on record keeping.

We do not have an internal audit department, but we conduct an internal audit every two years by three employees that work with unrelated department unless the Company determines that a longer rotation cycle is appropriate. The responsible employees and the audit are approved by the Company's board.

We periodically monitor changes in relevant applicable laws to stay updated and stay efficient in mitigating and preventing risks associated with money laundering and terrorist financing.

We have appointed the Compliance Officer.

1.14 Other Measures

Further, we implement the following measures:

- Implementation of written compliance policies and procedures;
- The assessment and documentation of money laundering and terrorist financing risks for the business, along with steps to mitigate those risks;
- Introduction of an ongoing compliance training plan;
- Establishing a plan for a review of the compliance program for the purpose of testing its effectiveness, and carrying out its review every two years at a minimum;
- Review of the compliance policies and procedures and risk assessment, and provision of tests of their effectiveness at least every two years;
- Appointment of a compliance officer.

1.15 Compliance Program

A compliance program is a program established and implemented by the Company and is intended to ensure their compliance under the PCMLTFA and associated regulations. A compliance program forms the basis for meeting all reporting, record keeping, client identification and other know-your-client requirements under the PCMLTFA and associated Regulations.

The Company implements the following elements of a compliance program by:

- appointing a compliance officer who is responsible for implementing the program;
- developing and applying written compliance policies and procedures that are kept up to date and, in the case of an entity, are approved by a senior officer;
- conducting a risk assessment business to assess and document the risk of a money laundering offence or a terrorist activity financing offence (ML/TF) occurring in the course of activities;
- developing and maintaining a written, ongoing compliance training program for employees, agents or mandatories, or other authorized persons;
- instituting and documenting a plan for the ongoing compliance training program and delivering the training (training plan); and
- instituting and documenting a plan for a review of the compliance program for the purpose of testing its effectiveness, and carrying out this review every two years at a minimum (two-year effectiveness review).

1.16 Penalties for violations

a) Administrative penalties

The Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (AMP Regulations) list the non-compliance violations that could be the basis of an AMP. The AMP Regulations categorize violations by degree of importance, and assign the following penalty ranges:

Minor violation	From CAD 1 to CAD 1,000 per violation
Serious violation	From CAD 1 to CAD 100,000 per violation
Very serious violation	From CAD 1 to CAD 100,000 per violation for an individual From CAD 1 to CAD 500,000 per violation for an entity

Multiple violations can result in a total amount that exceeds these limits.

b) Criminal penalties

FINTRAC may disclose cases of non-compliance to law enforcement when there is extensive non-compliance or little expectation of immediate or future compliance. Criminal penalties may include the following:

- Failure to report suspicious transactions: up to CAD 2 million and/or 5 years imprisonment.
- Failure to report a large cash transaction or an electronic funds transfer: up to CAD 500,000 for the first offence, CAD 1 million for subsequent offences.

- Failure to meet record keeping requirements: up to CAD 500,000 and/or 5 years imprisonment.
- Failure to provide assistance or provide information during compliance examination: up to CAD 500,000 and/or 5 years imprisonment.
- Disclosing the fact that a suspicious transaction report was made, or disclosing the contents of such a report, with the intent to prejudice a criminal investigation: up to 2 years imprisonment.

Penalties do not apply to those employees who report suspicious transaction to their senior employees.

2. Reporting Procedures

The information provided above forms our policies and procedures on identifying reportable transactions and reporting to FINTRAC, record keeping, record retention and ascertaining identity, risk-based approach, and training program.

2.1 Reporting to FINTRAC

As discussed in the previous section, the Company reports the following:

- Suspicious transaction
- Large cash transaction
- Terrorist property
- Electronic funds transfer
- Large virtual currency transactions

The Company will submit to FINTRAC a terrorist property report (TPR) detailing all property in their possession or control that the Company has reason to believe is owned, held or controlled by or on behalf of a terrorist group/listed terrorist person.

The Company will also report separately each transaction where it receives an amount of CAD 10,000 or more in cash in the course of a single transaction. Each such transaction will be sent to FINTRAC separately, in its own report. Finally, the Company will also report situations where the aggregate of multiple transactions with a 24-hour period, conducted by and/or on the behalf of the same person, entity, or beneficiary, is equal to or greater than CAD 10,000.

2.2 Enrolment with FINTRAC's electronic reporting system

The Compliance officer is responsible to ensure the Company is enrolled with FINTRAC's electronic reporting system, F2R system, to report electronically. Upon successful enrolment, the Company receives an identifier number to be included in the reports. The Compliance officer will retain and use the identifier number.

All reports submitted to FINTRAC shall be complete and accurate. The Compliance officer is responsible to ensure that the reports comply with all applicable laws.

To access to FINTRACT web reporting: https://fintrac-canafe.canada.ca/reporting-declaration/info/f2r-eng

Email: F2R@fintrac-canafe.gc.ca
1-866-346-8722

2.3 Procedure on Suspicious Transaction Reporting (STR)

Procedures — All employees are required to report any suspicious transactions to the Compliance officer as soon as first suspected. The Compliance officer files all suspicious transaction reports with FINTRAC and informs senior management of all suspicious transaction reports. Copies of the reports submitted, and the acknowledgement received in return from FINTRAC must be retained in a secure location.

The Compliance officer must submit STRs to FINTRAC electronically. Alternatively, if the Compliance officer does not have the technological capacity to send an STR electronically, he/she must submit it by paper.

There are two options for electronic reporting that provide for secure encrypted transmission that ensures the data's confidentiality and integrity. These two electronic reporting options are listed below:

- FINTRAC web reporting: https://www.fintrac-canafe.gc.ca/reporting-declaration/info/f2r-eng
- Batch reporting: https://www.fintrac-canafe.gc.ca/reporting-declaration/info/batch-lots-eng

FINTRAC web reporting is a secure application accessed through the internet that allows the Company to manually submit individual reports, as well as correct them if needed.

Batch reporting is a secure process that allows for the submission and correction of multiple reports (up to 10,000) in 'Batch files' that are formatted according to FINTRAC's specifications.

FINTRAC's STR paper reporting forms can be printed from the FINTRAC's reporting forms webpage: https://www.fintrac-canafe.gc.ca/reporting-declaration/form/form-eng

There are two ways to send a report to FINTRAC in such a way as to obtain an acknowledgement of receipt of a paper report:

Fax: 1-866-226-2346; or

Registered mail to the following address:

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

In addition, it is possible to send the report by regular mail to the FINTRAC address above.

2.4 Information to be contained in STR:

A variety of information is often collected as part of an assessment to be included in the report to FINTRAC. A well-completed STR should consider the following questions:

a) Who are the parties to the transaction?

- List the conductor, beneficiary, and holders of all accounts involved in the transaction;
- Take reasonable measures to identify the conductor of the transaction. This means that it is necessary to ask the client for this information unless there is an allegation that it may tip them off to the suspicion;

- Provide identifying information on the parties involved in the transaction. This could include the information recorded to identify the conductor, as well as any information on the other parties to the transaction or its recipients;
- List owners, directors, officers and those with signing authority, when possible. If the transaction involves a business, it is possible to include information on the ownership, control, and structure of the business in the STR.
- Provide clear information about each individual or entity's role in each of the financial transactions described.
- Explain the relationships among the individuals or entities (if known). This is very helpful to FINTRAC when trying to establish networks of individuals or entities suspected of being involved in the commission or attempted commission of an ML/TF offense.

b) When was the transaction(s) completed/attempted? If it was not completed, why not?

- Provide the facts, context, and ML/TF indicators regarding the transaction.

c) What are the financial instruments or mechanisms used to conduct the transaction?
d) Where did this transaction take place?
e) Why the transaction(s) or attempted transaction(s) are related to the commission or attempted commission of an ML/TF offense?

- State the ML/TF indicators used to support the suspicion.
- State the suspected criminal offense related to ML/TF, if known.

f) How did the transaction take place?

The reporting should be kept as long as the suspicion remains. It is required to periodically re-assess the client to verify that the level of suspicion has not changed. This process may be part of the Company's documented risk based approach or ongoing monitoring.

It is required to keep a copy of all STRs submitted to FINTRAC for at least 5 years from the date the report was submitted.

2.5 Procedure on large cash transaction reporting

When the client pays CAD 10,000 or more in cash, either in a single transaction or in multiple transactions, within a 24-hour period the Compliance Officer must submit the large cash transaction report within 15 calendar days.

Please follow the FINTRAC's guidance on the large cash transaction reporting at https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/Guide7A/lctr-eng

The copy of the submitted report should be kept within 5 years from the date the record was created.

2.6 Procedure on terrorist property reporting

Please follow the FINTRAC's guidance on the terrorist property reporting at: https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/guide5/5-eng

There are two ways to send a terrorist property report to FINTRAC in such a way as to obtain an acknowledgement of receipt of a paper report:

Fax: 1-866-226-2346; or

Registered mail to the following address:

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

The terrorist property report is only submitted on paper. It is not possible to send a report electronically at this time.

2.7 Procedure on non-SWIFT electronic funds transfer reporting

Upon sending or receiving instructions to transfer CAD 10,000 or more internationally, either in a single transaction or in multiple transactions, within a 24-hour period the Company must submit a report within 5 business days.

The Compliance Officer is required to submit non-SWIFT Electronic Funds Transfer Report electronically in accordance with the following FINTRAC's guidance: https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide8A/nseft-eng

The Compliance Officer needs to submit SWIFT Electronic Funds Transfer Report in accordance with the following FINTRAC's guidance: https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide8B/8b-eng

The Compliance Officer is required to submit non-SWIFT Electronic Funds Transfer Report by paper in accordance with the following FINTRAC's guidance: https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide8C/8c-eng

2.8 Procedure on large virtual currency transactions

When the Company receives virtual currency in an amount equivalent to CAD 10,000 or more in a single transaction, the Compliance Officer will submit a report to FINTRAC in accordance with the procedure set out below: https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/lvctr/lvctr-eng

3. Client information and record keeping

3.1 General

The Company performs record keeping under the PCMLTFA and associated regulations.

Depending on a particular business relationship, the Company may collect certain information from the client. Such information may include, for example:

- If an individual – full name, ID or passport details, date of birth, occupation, address, tax residency, source of origin of funds, employment details, purpose and intended use of the products and services, third party involvement, and any known political exposure

- If a legal entity – information on each beneficial owner, nature of business, information about company incorporation, certificate confirming existence, etc.

To verify the documents, the Company shall rely on the following guidance:
https://fintrac-canafe.canada.ca/guidance-directives/recordkeeping-document/record/msb-eng

3.2 Client information record

The Company retains client information for all clients who have a business relationship with the Company.

The Company completes client applications for payments products and services containing all of the required information, which depends on the type of client (individual or legal entity) and the nature and/or volume of the client's transactions. In particular, the records should contain:

- Client identification information (individual or legal entity)
- Industry, occupation, business type
- Beneficial ownership information (for legal entities)
- Third party determination and information
- Politically exposed person determination
- Business relationship information (purpose and intended use of the products and services)

3.3 What is beneficial ownership?

Beneficial owners are the actual 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 a corporation or an entity other than a corporation or trust, such as a partnership. The ultimate beneficial owners cannot be another corporation or entity; they must be the actual individuals who are the owners or controllers of the entity. In order to determine who the beneficial owners are, it is required to search through as many levels of information as necessary in order to determine the actual individuals.

It is important to consider that the names found on legal documentation may not be the actual owners of an entity. For example, legal owners of a corporation, entity, or trust may not be the actual individuals who own or control the corporation, entity, or trust.

That is why it is vital to identify beneficial ownership to remove anonymity and identify the actual individuals behind the transactions and account activities, which is a key component of Canada's anti-money laundering and anti-terrorist financing regime. The concealment of the beneficial ownership information of accounts, businesses, and transactions is a technique used in money laundering and terrorist activity financing schemes. Collection and confirmation of this information is an important step to aid in money laundering and terrorist activity financing investigations and ultimately protect the integrity of Canada's financial system.

3.4 How to obtain information about beneficial owners?

Beneficial ownership information, as well as the ownership, control, and structure information, should be obtained from the Client, either verbally or in writing.

For example:

- the Client can provide with official documentation to confirm information
- the Client can refer to publicly available records to confirm information
- the Client can inform about the beneficial ownership information which should be written down for record-keeping purposes or
- the Client can fill out an application form with the relevant information included

In all cases it is information on the actual individuals who are the beneficial owners as well as information establishing the entity's ownership, control, and structure that must be obtained.

All documents should be accurately retained in the client's file. If necessary, it is required to search through as many levels of information in order to determine beneficial ownership. If there is no individual who owns or controls 25% or more, then the Compliance Officer must still keep a record of the information obtained.

The Compliance Officer is not required to identify senior managing officers if there is no individual who owns or controls 25% or more. Still, the Compliance Officer will need to retain the name of individuals who have a managing role or control over a percentage of shares that the Compliance Officer determines to be significant, even if it is less than 25%.

If the client refuses or fails to provide the requested information, the client shall be considered high risk, and enhanced due diligence is required. The Company may decide to refuse to proceed with doing business with this client.

For more clarification, please follow this FINTRAC's Guidance: https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/bor-eng

3.5 What is a third party? How is it determined?

A third party is a person or entity who instructs another person or entity to conduct an activity or financial transaction on their behalf. When determining whether a third party is giving instructions, it is not about who owns or benefits from the money, or who is carrying out the

transaction or activity, but rather about who gives the instructions to handle the money or conduct a transaction or particular activity. If the client is acting on someone else's instructions, that someone else is the third party.

When a person is acting on behalf of their employer, the employer is considered to be the third party, unless the person is making a cash deposit to the employer's business account.

The PCMLTFA and associated Regulations require to take reasonable measures to make a third party determination for certain transactions and activities. Once the determination is made, it is required to identify and record the third party involved in any transaction reported to FINTRAC.

The Financial Action Task Force (FATF), FINTRAC, Egmont, and other anti-money laundering and anti-terrorist financing authoritative bodies have observed the use of third parties in several money laundering and terrorist financing cases. It is not uncommon for criminals to use third parties as a method to evade detection by distancing themselves from the proceeds of crime.

Third party determination

It is required to take reasonable measures to determine if there is a third party who is instructing the client to conduct an activity or a transaction.

Reasonable measures include asking the client if they are acting on someone else's instructions, or by retrieving the information already contained in the Company's records.

The Compliance Officer will need to document the information on applications and forms. If there is a third party involved, required information about the third party is also recorded on applications and forms such as:

- Name and address of third party
- Occupation or principal business of third party
- Date of birth (for individuals)
- Registration number and place of incorporation (for legal entities)
- Nature of relationship between third party and client

If there are reasonable grounds to suspect that there is a third party involved the Company records such information in client files. Further it is necessary to indicate:

- Whether the transaction is conducted on behalf of a third party
- Reasons why the Company suspects the individual acting on behalf of a third party

3.6 Who is a politically exposed person (PEP)?

Foreign PEP

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

- head of state or head of government;

- member of the executive council of government or member of a legislature;
- deputy minister or equivalent rank;
- ambassador, or attaché or counsellor of an ambassador;
- military officer with a rank of general or above;
- president of a state-owned company or a state-owned bank;
- head of a government agency;
- judge of a supreme court, constitutional court or other court of last resort; or
- leader or president of a political party represented in a legislature.

These persons are foreign PEPs regardless of citizenship, residence status or birth place.

A person determined to be a foreign PEP, is forever a foreign PEP.

Domestic PEP

A domestic PEP is a person who holds — or has held within the last 5 years — a specific office or position in or on behalf of the Canadian federal government, a Canadian provincial government, or a Canadian municipal government:

- Governor General, lieutenant governor or head of government;
- member of the Senate or House of Commons or member of a legislature;
- deputy minister or equivalent rank;
- ambassador, or attaché or counsellor of an ambassador;
- military officer with a rank of general or above;
- president of a corporation that is wholly owned directly by Her Majesty in right of Canada or a province;
- head of a government agency;
- judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
- leader or president of a political party represented in a legislature; or
- mayor.

Mayor: in line with legislation across Canada, municipal governments include cities, towns, villages, and rural (county) or metropolitan municipalities. As such, a mayor is the head of a city, town, village, or rural or metropolitan municipality, regardless of the size of the population.

A person ceases to be a domestic PEP 5 years after they have left office.

A PEP also includes close associates and family members, such as:

- mother and father
- children
- spouse or common-law partner
- spouse's or common-law partner's mother or father
- brother, sister, half-brother, or half-sister (that is, any other child of the individual's mother or father)

3.7 Who is the head of international organization?

The head of an international organization is a person who is either:

- the head of an international organization established by the governments of states; or
- the head of an institution established by an international organization.

The head of an international organization or the head of an institution established by an international organization means the primary person who leads that organization, for example a president or CEO.

There is no requirement for an institution established by an international organization to operate internationally. It is possible that an institution that has been established by an international organization only operates domestically, or in one jurisdiction.

The Compliance Officer should use reasonable measures to determine if the person is the head of an international organization or the head of an institution set up by an international organization.

Once a person is no longer the head of an international organization or the head of an institution established by an international organization, that person is no longer a HIO.

Procedure

If the Company determines that the person is a foreign PEP, or a family member or close associate of a foreign PEP, the Compliance Officer takes reasonable measures to establish the source of the funds deposited or expected to be deposited and obtain senior management approval to establish the business relationship with the client. As a high-risk client, the person must be subject to the Company's policies and procedures for high-risk clients.

3.8 What is a business relationship?

A business relationship is a relationship established between the Company, as a reporting entity, and a client to conduct financial transactions or provide services related to those transactions.

Business relationships are established once a client has an account with the Company. If the client does not have an account with the Company, a business relationship is formed when the client has conducted two or more transactions or activities through the Company, for which the Company is required to:

- verify their identity of the individual, or
- confirm the existence of the entity.

Once the business relationship is established, the Compliance Officer is responsible for:

- Keeping a record of the purpose and intended nature of the business relationship
- Conducting ongoing monitoring of the business relationship with the client in order to (i) detect any transactions that need to be reported as suspicious, (ii) keep client identification and beneficial ownership information, as well as the purpose and intended nature records up-to-date, (iii) reassess clients risk level based on their transactions and activities, (iv) determine if the transactions and activities are consistent with the information held about the client.

- Keeping a record of the measures taken to monitor the business relationship and the information obtained.

3.9 What is enhanced due diligence?

The enhanced due diligence measures for high risk clients include:

- gathering additional information about the client (e.g. connected parties, accounts, or relationships), its beneficial owner and updating more regularly the client profile, including the identification data;
- gathering additional information on the planned substance of the business relationship;
- gathering information on the origin of the funds and wealth of the customer and its beneficial owner;
- gathering information on the underlying reasons of planned or executed transactions
- receiving permission from the senior management of the Company to establish or continue a business relationship;
- improving the monitoring of a business relationship by increasing the number and frequency of the applied control measures and by choosing transaction indicators that are additionally verified;
- demanding a customer make a payment from an account held in the customer's name in a credit institution of a contracting state;
- preparing an investigation report with the use of enhanced due diligence software and agencies.

Some examples of documents and information required for enhanced due diligence:

For Businesses and other legal entities:

- Official corporate records from company's management;
- Registration documents from the local Registrar of Companies;
- Articles of incorporation, partnership agreements, and business certificates;
- Names and locations of its customers and suppliers;
- Banking information and relationships with other financial institutions;
- Identity of board members and beneficiaries;
- Basic details on corporate history and structure;
- Standard documents, which confirm the sale of property, inheritance, salary, etc.;
- AML policies and procedures in place;
- Third-party documentation;
- Information on Local market reputation through review of media sources.

For all high-risk individuals and beneficial owners of high risk clients:

- Documents showing income or source of wealth (copy of the most recent tax return, bank account statement);
- Reference letter from bank, lawyer or auditor;
- CV

Additionally, For Politically exposed persons (PEP):

- Title and details on the position the PEP holds or held. This includes the level of influence of the position;
- If the PEP is a close associate or family member, their identity, title, role, and level of proximity to public office should be established;
- Documents showing salary.

All high-risk customers are subject to a minimum annual review.

The Company also takes into consideration all relevant adverse information. Whether an official document or something posted publicly on the Internet, any information that pertains to money laundering or corruption is thoroughly considered.

The Company may conduct an on-site visit to the physical address. Documents that cannot be provided digitally can be verified physically. A risk-based threshold is breached if the physical address does not correspond with the address stated on official documents.

The enhanced due diligence measures when we deal with a politically exposed person are:

- obtaining approval from the senior management of the Company to establish or continue a business relationship with the person and making sure that only senior management of the Company gives approval for a new business relationship;
- applying measures to establish the origin of the wealth of the person and the sources of the funds that are used in the business relationship or upon making occasional transactions;
- monitoring the business relationship in an enhanced manner.

4. Sanction Policy

The Company does not enter into any transaction with individuals, companies and countries that are on prescribed sanctions lists.

The Company will therefore screen against:

1. US Consolidated Sanctions,
2. OFAC - Specially Designated Nationals (SDN),
3. EU Financial Sanctions,
4. UK Financial Sanctions (HMT),
5. Australian Sanctions,
6. Switzerland Sanctions List – SECO,
7. Interpol Wanted List,
8. Consolidated Canadian Autonomous Sanctions List,
9. Office of the Superintendent of Financial Institutions (Canada),
10. Bureau of Industry and Security (US),
11. Department of State, AECA Debarred List (US),
12. Department of State, Nonproliferation Sanctions (US),
13. other lists,

in all jurisdictions in which we operate.

4.1 Non-Face-to-Face Customers

The Company will apply equally effective customer identification procedures and ongoing monitoring standards for non-face-to-face customers for identification purposes as for those where the customer is available for interview. If a customer is not physically present for identification purposes, the Company will additionally obtain:

- additional information on the customer;
- additional information on the intended nature of the business relationship;
- information on the source of funds or source of wealth of the customer;
- information about the reasons for the intended or performed transactions;
- approval from senior officer for establishing business relationships.

In course of a future business relationships the Company will conduct enhanced monitoring of the relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further explanation.

In case of any suspicion or any lack on client information or documents, the Company will proceed with online video streaming to confirm their identity.

In case of non-face-to-face clients the Company will also require that the first payment is made through an account in the customer's name with a financial institution which is a subject to similar CDD standards.

The Company accepts only duly certified copies of documents and will not accept documents which have been self-certified by the customer.

4.2 Record Keeping

Pursuant to the PCMLTFR, the Company will comply with the record keeping requirements. It will maintain detailed records of the following:

- a copy of every report sent to FINTRAC (suspicious transaction reports; terrorist property reports; large cash transaction reports);
- large cash transaction records;
- records of transactions of CAD 3,000 or more;
- records of remitting and transmitting CAD 1,000 or more in funds by means other than an electronic funds transfer;
- records of electronic funds transfers of CAD 1,000 or more; and
- foreign currency exchange transaction tickets;
- records of virtual currency transfers equivalent to CAD 1,000 or more,
- virtual currency exchange transaction tickets,
- crowdfunding platform services records,
- created or received internal memorandums about MSB services,
- service agreement records.

A record of transactions should include the date as well as name, address, date of birth, and occupation of the person making the transaction. If the transaction was made by an entity it should also include its name, address, and nature of its principal business.

All documents and records mentioned above are kept throughout the business relationship with the customer and for a period of at least five years after the end of the business relationship.

4.3 Travel Rule

As per the travel rule, the Company will obtain specific information related to an electronic fund transfer (“ETF”) or virtual currency (“VC”) transfer . The travel rule applies when a financial entity receives or transmits an ETF or VC.

The required information for ETFs includes:

- the name, address and account number or other reference number (if any) of the person or entity who requested the ETF;
- the name and address of the beneficiary and recipient of the ETF; and
- the beneficiary's account number or other reference number.

When sending an incoming or outgoing EFT (after receiving it as an intermediary), the Company must include the travel rule information received or obtained through reasonable measures.

The required information for ETFs includes:

- the name, address and the account number or other reference number (if any) of the person or entity who requested the transfer (originator information); and
- the name, address and the account number or other reference number (if any) of the beneficiary.

4.4 Correspondent banking relationships

Where the Company has a correspondent banking relation (financial arrangements or agreements) with a foreign financial institution, it will take necessary steps to verify information and records of the foreign financial institution, ensure that the foreign financial institution is not a shell bank, set out its obligations towards the foreign financial institution in writing, and take steps to determine that the foreign financial entity has not been liable for criminal or civil penalties in respect to money laundering.

5. Client verification and confirmation of the existence

The requirement to verify the identity of an individual and confirm the existence of a corporation or of an entity other than a corporation under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations applies to all reporting entities (REs).

5.1 How do I verify the identity of an individual?

There are three ways to verify the identity of an individual:

Government-issued photo identification method where 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;
- match the name and appearance of the person being identified.

It is possible to verify a document using a credit or dual-process method:

- Credit file method where the information must be valid and current; or
- Dual-process method where the information must be:
    - valid and current; and
    - from different sources.

a) Government-issued photo identification document method

A government-issued photo identification document must be issued by either a federal, provincial or territorial government in order to be used to verify the identity of an individual. It is possible to accept a foreign government-issued photo identification document if it is an equivalent to a Canadian document. Photo identification documents issued by municipal governments, Canadian or foreign, are not acceptable.

The photo identification document must:

1. indicate the individual's name;
2. include a photo of the individual;
3. include a unique identifying number; and
4. match the name and appearance of the individual being identified.

To determine the authenticity of a government-issued photo identification document in person it is necessary to check the characteristics of the original physical document and its security features (or markers, as applicable) in the presence of the individual to be satisfied that it is authentic as issued by the competent authority (federal, provincial, territorial government) that is valid (unaltered, not counterfeit) and current (not expired).

If an individual is not physically present, the authenticity of a government-issued photo identification document must be determined by using a technology capable of assessing the document's authenticity. For example:

- an individual could be asked to scan their government-issued photo identification document using the camera on their mobile phone or electronic device; and
- a technology would then be used 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, territorial government).

When an individual is not physically present, the government-issued photo identification document needs to match the name and photo of the person in the authenticated document provided. For example:

- An individual could participate in a live video chat session and the Company would then be able to 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
- An individual could be asked to take a "selfie" photo using the camera on their mobile phone or electronic device, and an application would apply facial recognition technology to compare the features of that "selfie" to the photo on the authentic government-issued photo identification document. A process would have to exist to also compare the name on the government-issued photo identification document with the name provided to the Company by the individual.

Note: It is not enough to just view a person and their government-issued photo identification document online through a video conference or any other type of virtual application. It is required to use a software or some type of technology that would be able to authenticate the government-issued photo identification document. Further, it is necessary to verify that the name and image match that of the individual on the authentic government-issued photo identification document.

The Compliance Officer should follow internal policies and procedures that describe the processes to authenticate a government-issued photo identification document, whether in person or not, and the confirmation that it is valid and current.

The processes to determine that a government-issued photo identification document is authentic, valid and current, and the verification step (ensuring that the name and picture matches the name and face of the person), do not need to happen concurrently.

What information needs to be recorded when using the government-issued photo identification document method?

When using the government-issued photo identification document method, it is required to record:

- the individual's name;
- the verification date of the individual's identity;
- the type of document used (for example, driver's license, passport, etc.);
- the unique identifying number of the document used;
- the jurisdiction (province or state) and country that issued the document; and
- the expiry date of the document, if available (to record if the information appears on the document or card).

b) Credit file method

To be deemed an acceptable method, the credit file must:

- be from a Canadian credit bureau (credit files from foreign credit bureaus are not acceptable);
- have been in existence for at least three years; and
- match the name, address and date of birth that the individual provided.

A credit file provides a rating on an individual's ability to repay loans; however, it is possible to request a credit file to verify an individual's identifying information that does not include a credit assessment. Credit assessment is needed to verify the identity of an individual. Equifax Canada and TransUnion Canada are Canadian credit bureaus that provide credit file information for identification purposes.

To rely on the credit file method, it is necessary to conduct the search at the time of verifying the individual's identity. Copies of credit files or previously obtained credit file cannot be used.

It is acceptable to use an automated system to match the individual's information with the information contained in the individual's credit file. A third party vendor needs to provide with valid and current information contained in the individual's credit file. A third party vendor is an entity that is authorized by a Canadian credit bureau to provide access to Canadian credit information.

If any of the information provided by the individual (name, address, or date of birth) does not match the information in the credit file, that credit file cannot be used to verify the identity of this individual. The Company will need to use another source or method to verify the individual's identity.

On occasion, information found within the credit file may contain a variation of the name or a discrepancy in the address that was provided by the individual. In these instances, the information in the credit file is compared against the information collected from the individual. For example:

- If there is a slight typo in the address or name, it is necessary to determine that the information still matches what the individual provided.
- If there is a discrepancy in their date of birth, it is more likely that the information does not match.

In this case, if this is the Company’s determination, it is not possible to rely on the information referred to in the credit file for identification purposes. An alternative source or

method (government-issued photo identification document or dual process) to verify the individual's identity must be used.

- If there are multiple addresses in the credit file, it is possible that the address that the individual provided is not the primary address in the credit file but does appear in the credit file as a secondary address. It is possible that this may still meet the Company's requirements for ensuring that the information matches what the individual provided.

What information needs to be recorded when using the credit file method?

In this method the following information is recorded:

- the individual's name;
- the date the Company consulted or searched the credit file;
- the name of the Canadian credit bureau or third party vendor holding the credit file; and
- the individual's credit file number.

c) Dual-process method to verify the identity of an individual

It is possible to verify the identity of an individual using the dual-process method. This method involves referring to information from reliable sources.

How to use the dual process method to verify the identity of an individual

To verify an individual's identity by using the dual-process method, the Company must refer to any two of the following:

- information from a reliable source that includes the individual's name and address;
- information from a reliable source that includes the individual's name and date of birth; or
- information that includes the individual's name and confirms that they have a deposit account, credit card or other loan account with a financial entity.

Information for this purpose may be found in statements, letters, certificates, forms or other sources and can be provided through an original version or another version of the information's original format, such as a fax, photocopy, scan, or electronic image. For further clarity, it is acceptable to rely on a fax, photocopy, scan or electronic image of a government-issued photo identification document as one of the two sources of information required to verify the identity of an individual.

The information obtained must originate from two different sources and cannot come from the individual whose identity is being verified nor can it come from the person or entity doing the verification. The name, address, date of birth or confirmation of a deposit account, credit card or other loan account must match the information that was provided by the individual.

Note: It is not acceptable to rely on information if the account number or number that is associated with the information is truncated or redacted. On occasion, information contained in a source may contain a variation of the name or a typo in the address. In these instances, it is necessary to determine whether the information matches the information collected from the

individual. If it is a slight typo in the address or a misspelled name, it is required to determine that the information still matches what the individual provided. However, in the case of an incorrect date of birth, it is more likely that that the information does not match. In this case, it is not possible to rely on the information referred to in these two sources for identification purposes. An alternative source or method (government-issued photo identification or credit file) to verify the individual's identity must be used or obtained a different source under the dual process method.

It is not possible to use the same source for the two categories of information used to verify the individual's identity. For example, it is not possible to rely on a bank statement from Bank A that includes the individual's name and address and another bank statement from Bank A that includes the individual's name and confirms that the individual holds a deposit account, as Bank A would be the originating source of both categories of information. However, it is possible to refer to a bank statement from Bank A that contains the individual's name and confirms that the individual holds a deposit account, and rely on an electronic image of a driver's license to verify the individual's name and address. For further precision:

- refer to one reliable source to verify an individual's name and address, and refer to a different reliable source to verify their name and date of birth.
- refer to one reliable source to verify an individual's name and address, and refer to a different source to verify their name and confirm a financial account (specifically a deposit account, credit card account or loan account).
- refer to one reliable source to verify an individual's name and date of birth, and refer to a different source to verify their name and confirm a financial account (specifically, a deposit account, credit card account or loan account).

What is a reliable source of information?

A reliable source is an originator or issuer of information that the Company trusts. To be considered reliable, the source should be well known and considered reputable. For example, a reliable source could be the federal, provincial, territorial or municipal levels of government, crown corporations, federally regulated financial institutions, or utility providers.

Note: If the information (two of either of the following: name and address, name and date of birth, or name and confirmation of a deposit account, credit card or other loan account) obtained through the identification process does not match the information provided by the individual, the Company cannot rely on it. Social media of any kind is not an acceptable source of information to verify an individual's identity.

If the Company has already verified the identity of an individual, the Company does not need to re-verify it upon subsequent account openings or transactions, unless the Company has doubts about the accuracy of the information that was used at the time of verification.

How to use a credit file under the dual process method to verify the identity of an individual?

A Canadian credit file can be used as one of the two sources of information required to verify the identity of an individual. It can be used to verify the individual's name and address, name and date of birth, or to verify the individual's name and confirm that the individual has a

deposit account, credit card or loan account. The credit file must have existed for at least six months.

Information from a second source, for example, a property tax assessment, must be used to verify the second category of information under the dual process method. In this instance, the two reliable sources are the Canadian credit bureau that provided the credit file information and the municipal government that issued the property tax assessment. The information from these two sources must match the information provided by the individual.

The Company can rely on information from a Canadian credit bureau if it acts as an aggregator and if it compiles information from different reliable sources (often referred to as tradelines). In this instance, the Canadian credit bureau must provide with information from two independent tradelines that verify two of either: the individual's name and address, the individual's name and date of birth, or the individual's name and confirmation of a deposit account, credit card or loan account. In this instance, each tradeline is a distinct source; the credit bureau is not the source.

The tradelines cannot be the Company's own, as the reporting entity verifying the individual's identity, and each tradeline must originate from a different source (for example, federally regulated financial institution, utility service provider, etc.).

What information needs to be recorded when using the dual-process method?

There is specific information to be kept when this method is used to verify an individual's identity. The following information must be recorded:

1. the individual's name;
2. the date when the information is verified;
3. the name of the two different sources that were used to verify the identity of the individual;
4. the type of information consulted (for example, utility statement, bank statement, marriage licence); and
5. 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.).

If the Company receives two distinct sources from an aggregator of that information, the Company must record the tradeline account number or number associated to each tradeline, not the aggregator number.

How to confirm the existence of a corporation or of an entity other than a corporation?

An entity can be a corporation, trust, partnership, fund, or unincorporated association or organization. However, corporations are subject to different requirements than entities other than corporations.

Corporations

To confirm the existence of a corporation, the Company can refer to a paper record or an electronic record that was obtained from a source that is accessible to the public, such as:

- its certificate of incorporation;
- a certificate of active corporate status;
- a record that has to be filed annually under provincial securities legislation; or
- any other record that confirms the corporation's existence, such as 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.

The Company can obtain a corporation's name and address and the names of its directors from a provincial or federal database such as the Corporations Canada database, which is accessible from Innovation, Science and Economic Development Canada. To get this type of information the Company should subscribe to a corporation searching and registration service.

The Company must verify the corporation's name, address and the names of its directors. In the case of a corporation that is a securities dealer, the Company does not need to verify the names of its directors when the confirmation exists.

The Company does not have to re-confirm the existence of a corporation nor to verify the corporation's name, address and the names of its directors unless the Company has doubts about the accuracy of the information or the record used.

An entity other than a corporation

To confirm the existence of an entity, other than a corporation, the Company can refer to a paper record or an electronic record that was obtained from a source that is accessible to the public, such as:

- a partnership agreement;
- articles of association; or
- any other record that confirms its existence as a legal entity (for example, trust agreement).

The Company does not have to re-confirm the existence of an entity unless the Company has doubts about the accuracy of the information or the record used.

Records required when confirming the existence of a corporation or of an entity other than a corporation

If the Company refers to a publicly accessible electronic record to confirm the existence of a corporation or of an entity other than a corporation, the Company must keep a record of:

- the corporation's registration number or the entity's registration number;
- the type of record consulted; and
- the source of the electronic version of the record.

If the Company consults a paper record to confirm the existence of a corporation or of an entity other than a corporation, the Company must retain the record or a copy of the record.

Are there 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 Company has to inform clients about the collection of their personal information. However, the Company does not have to inform them when the Company includes their personal information in the reports the Company is required to submit to FINTRAC.

The Office of the Privacy Commissioner of Canada can provide further guidance, and has created a Question and Answer document about PIPEDA and the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, to help clarify the responsibilities under both federal Acts.

6. Risk based approach

6.1 Risk assessment

As part of the risk assessment, the Company conducts risk evaluation of the business, clients, and/or business relationships at least every 2 year in order to identify the areas that are vulnerable to being used by criminals for conducting money laundering or terrorist financing (ML/TF) activities.

The risk is assessed in accordance with the Company's Risk Scoring. The Company's vulnerabilities include weak controls within the Company that offer high risk products and services.

During the risk assessment, the following areas are examined:

- Products, services, and delivery channels;
- Geography risks;
- Clients and business relationships risks; and
- Other relevant factors.

Products, services, delivery channels

The Company begins its risk assessment by taking a business-wide perspective. The Company assesses all its products, services and delivery channels to determine if they pose a high risk of ML/TF. This may include, but is not limited to:

- Foreign exchange transactions
- Electronic funds transfers
- Issuing or redeeming money orders
- Non face-to-face services (Internet, mail or telephone), etc.

Additionally, it is necessary to consider the following:

- Assess the products and services by the type of client they are meant for (e.g. corporate, individuals, wholesale, retail, etc.)
- Do the products and services provided allow a client to engage in high-risk transactions? For example, can the Company's clients transfer funds on behalf of a third party?
- How does the Company provide its product? Do clients have to come to the Company's location to buy a product or service or can they conduct a transaction over the phone, by fax or online?

Some examples of potentially high-risk products, services and delivery channels are:

- Electronic funds transfers (EFTs) can pose a higher risk because they support the rapid movement and conversion of assets into, through and out of the financial system.
- Products offered through the use of agents. When a third party identifies clients on the Company's behalf, this may pose a greater risk as they may not be properly following policies and procedures.

- Offering products and services through non-face-to-face (phone, fax, online) means. These delivery channels may pose higher risks because it may be more difficult to identify the client.
- The business may be offering products and services that are based on new technologies such as electronic wallets, mobile payments, or virtual currencies. These may be considered higher risk as they can transmit funds more quickly or anonymously.

Geography

Geography location could pose a high risk for ML/TF activities. The factors that cannot increase a risk for ML/TF activities include:

- Proximity to high crime and rural areas, board-crossing, etc.
- Client connection to high risk countries
- Client can make anonymized payments using online exchange services
- Global clients are harder to identify due to the difference in procedures of how customer identification documents are obtained and what they contain

Other factors

There can be other factors that do not fall in previous categories. Additional factors to be assessed within the operation of the Company's business include: a client uses false or fictious documents, use of anonymized wallets, transfers from countries with higher money laundering risks.

What are the high risk factors?

Risk level of the client is determined based on the Risk Scoring, unless there are factors that on their own indicate that the client is a high risk regardless of other factors. The Company considers a client as a high risk if:

- a client is PEP/HIO or close associate
- a client commits a suspicious transaction and we have received a request for Information from Law Enforcement, Regulators etc.
- MLRO and Senior Management Request (based on internal investigations etc.)

Mitigation measures

For high risk clients the Company shall use mitigation measures, including:

- identification of all clients without exceptions in accordance with CDD and EDD requirements,
- no anonymous transactions are allowed,
- depositing the client's wallet from known sources,
- performing enhanced monitoring of transactions and business relationships,
- obtaining additional information beyond the minimum requirements about the intended nature and purpose of the business relationship, including the type of business activity,

- monitoring transactions on a constant basis to be conducted by Company's internal control system,
- obtaining and retaining client and transaction records for at least 5 years,
- no transactions are allowed with entities located in countries without adequate AML/CTF controls,
- setting transaction limits to avoid AML and CTF risks.

7. Effectiveness review and plan

7.1 Requirements related to two-year effectiveness review and plan.

A two-year effectiveness review is an evaluation that must be conducted every two years (at a minimum) to test the effectiveness of the elements of the Company's compliance program (policies and procedures, risk assessment, and ongoing training program and plan).

The Company must start the effectiveness review no later than two years (24 months) from the start of the previous review and must also ensure that the Company has completed the previous review before starting the next review.

The purpose of an effectiveness review is to determine whether the Company's compliance program has gaps or weaknesses that may prevent the business from effectively detecting and preventing ML/TF.

The effectiveness review will help the Company to determine if:

- the Company's business practices reflect what is written in its compliance program documentation and if the Company is meeting the requirements under the PCMLTFA and associated Regulations.
- the Company's risk assessment is effective at identifying and mitigating the ML/TF risks related to its clients, affiliates (if any), products, services, delivery channels, new developments or technology, and geographic locations where the Company does business.

7.2 Who can conduct the effectiveness review.

The review must be carried out and the results documented by an internal or external auditor, or by The Company in the case when the Company does not have an auditor. The review should be conducted by someone who is knowledgeable of the Company's requirements under the PCMLTFA and its associated Regulations. Also, as a best practice, to ensure that the review is impartial, it should not be conducted by someone who is directly involved in the Company's compliance program activities. Regardless of who carries out the review, as an result it is the Company's responsibility to ensure that the review is conducted (at a minimum) every two years and that the review tests the effectiveness of the Company's compliance program.

7.3 Effectiveness plan

The Company must also institute and document a plan for the two-year effectiveness review of its compliance program. This plan should describe the scope of the review and must include all the elements of the Company's compliance program. The breadth and depth of review for each element may vary depending on factors such as the complexity of the Company's business, transaction volumes, findings from previous reviews, and current ML/TF risks. The plan should not only describe the scope of the review, but it should include the rationale that supports the areas of focus, the time period that will be reviewed, the anticipated evaluation methods and sample sizes.

7.4 The evaluation methods of effectiveness review

The evaluation methods can include, but are not limited to, interviewing staff, sampling records and reviewing documentation. The following are examples of what can be included in the review:

- interviews with those handling transactions to evaluate their knowledge of the Company's policies and procedures and related record keeping, client identification and reporting requirements;
- a review of a sample of the Company's records to assess whether the client identification policies and procedures are being followed;
- a review of the Company's agreements with agents or mandataries, as applicable, as well as a review of a sample of the information that the Company's agents or mandataries referred to in order to verify the identity of persons, to assess whether client identification policies and procedures are being followed;
- a review of transactions to assess whether suspicious transactions were reported to FINTRAC;
- a review of large cash transactions to assess whether they were reported to FINTRAC with accurate information and within the prescribed timelines;
- a review of electronic funds transfers to assess whether reportable transfers were reported to FINTRAC with accurate information and within the prescribed timelines (applicable to RE sectors that have EFT obligations);
- a review of a sample of the Company's client records to see whether the risk assessment was applied in accordance with your risk assessment process;
- a review of a sample of the Company's client records to see whether the frequency of ongoing monitoring is adequate and carried out in accordance with the client's risk level assessment;
- a review of a sample of high-risk client records to confirm that enhanced mitigation measures were taken;
- a review of a sample of the Company's records to confirm that proper record keeping procedures are being followed;
- a review of the Company's risk assessment to confirm that it reflects the current operations; and
- a review of the Company's policies and procedures to ensure that they are up to date and reflect the current legislative requirements and that they reflect your current business practices.

7.5 Documentation of two-year effectiveness review

The Company should also document the following in its two-year effectiveness review:

- the date the review was conducted, the period that was covered by the review and the person or entity who performed the review;
- the results of the tests that were performed; and
- the conclusions, including deficiencies, recommendations and action plans, if any.

The Company must report, in writing, the following to a senior officer no later than 30 days after the completion of the effectiveness review:

- the findings of the review (for example, deficiencies, recommendations, action plans);

- any updates made to the policies and procedures during the reporting period (the period covered by the two-year review) that were not made as a result of the review itself; and
- the status of the implementation of the updates made to the Company's policies and procedures.

8. Ongoing training program

All individuals within the Company who:

- contact with client,
- see client transaction activity,
- handle transaction of funds,
- are responsible for implementing and overseeing the compliance regime,

are required to pass the training program to learn and understand about their obligations.

All new employees that communicate with clients complete the training on the first date of employment, while other employees are trained annually or more frequently in case of any legislation changes or new policies.

They need to know and understand, including:

1. the Company's own personal statutory obligations and the possible consequences for failure to report suspicious transactions;
2. any other statutory and regulatory obligations that concern the Company under the PCMLTFA, and the possible consequences of breaches of these obligations;
3. the Company's policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting;
4. any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by the staff and other personals to carry out their particular roles in the Company with respect to AML/CFT.

The training is assigned for all employees, agents, mandatories, or other persons authorized to act on the Company behalf:

1. all new staff, irrespective of seniority;
2. to the Compliance Officer;
3. back-office staff, depending on their roles;
4. managerial staff,
5. agents,
6. mandatories,
7. other persons authorized to act on the Company behalf.

Training program provides all personals with an understanding of the process of money laundering, the laws and regulations that make it illegal, and the responsibilities of employees to help detect and prevent it.

The training on AML/CFT issues raises awareness of financial crime risks, global laws and regulations, laws and regulations applicable the Company.

General training program designed for all operational staff includes:

1. general information: the background and history pertaining to money laundering controls, what money laundering and terrorist financing is;

2. legal framework: how AML/CFT laws and regulations apply to the Company and its employees;
3. penalties for anti-money laundering violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment;
4. how to react when faced with a suspicious client or activity;
5. internal policies, such as customer identification and verification procedures and CDD policies;
6. what the legal record keeping requirements are;
7. suspicious activity reporting requirements;
8. duties and accountability of employees.

Training is delivered annually. Additional training is provided regularly to all employees based on, but not limited to, changes in government regulations and the Company's compliance program requirements.

The Company uses mix of training techniques and tools in delivering training, depending on the available resources and learning needs of its staff. These techniques and tools include online learning systems, focused classroom training, relevant videos as well as paper- or intranet-based procedures manuals. The Company also includes available FATF papers and typologies as part of its the training materials. All materials are kept up-to-date and in line with current requirements and standards. Instructors can be in-house personnel or an external service provider, but they should have knowledge of the PCMLTFA and associated Regulations.

Training program includes a record of the training that has been delivered (the date the training took place, a list of the attendees who received the training, the topics that were covered). The Company will keep the staff training records for at least 3 years after the training session has been completed.

Training program completion

Employee (Name, Surname)	Training name, description and content	Completion date	Employee's signature

9. Money Laundering Compliance Officer

Compliance Officer is the Company's employee responsible for overseeing all activity related to anti-money laundering matters.

The Compliance Officer is responsible for regular monitoring of applicable laws so that the Company is updated with the recent developments and controls money laundering and terrorism financing risks. In particular, the Compliance Officer's responsibilities include:

- Receiving disclosures from employees (also known as Suspicious Transaction Report STR's);
- Deciding if disclosures should be passed on to the Financial Transactions and Reports Analysis Centre or the Royal Canadian Mounted Police (RCMP) or the Canadian Security Intelligence Service (CSIS);
- Reviewing all new laws and deciding how they impact on the operational process of the company;
- Preparing a written procedures manual and making it available to all staff and other stakeholders;
- Making sure appropriate due diligence is carried out on customers and business partners;
- Receiving internal Suspicious Transaction Report (STR) from staff;
- Deciding which internal STR's need to be reported on to FINTRAC or RCMP or CSIS;
- Recording all decisions relating to STRs appropriately;
- Ensuring staff receive anti-financial crime training when they join and that they receive regular refresher training;
- Monitoring business relationships and recording reviews and decisions taken;
- Making decisions about continuing or terminating trading activity with particular customers;
- Making sure that all business records are kept for at least five years from the date of the last customer transaction as per FINTRAC regulations.

The Compliance Officer should remain completely independent and rely on applicable laws when taking necessary decisions. Senior management or other employees should not influence of the decisions taken by the Compliance Officer within the scope of its responsibility.

Company's Compliance Officer:

Name: [Full Name]

Title: [Title]

Signature: _____

Date:

Approved by:

Name: [Full Name]

Title: [Title]

Signature: _____

Date:

Please familiarize yourself with the Company's Compliance Officer.

In the absence of the Compliance Officer, Supporting Compliance Officers will take his/her place.

Company's Supporting Compliance Officer:

Name: [Full Name]

Title: [Title]

Signature: _____

Date:

Approved by:

Name: [Full Name]

Title: [Title]

Signature: _____

Date: