ANTI-MONEY LAUNDERING POLICY AND PROCEDURE

Table of Contents

1 POLICY STATEMENT

GPG (GLOBAL PROCESSING GROUP) (hereinafter referred to as "the Company", "we", "us", or "our") is committed to the highest standards of anti-money laundering and countering the financing of terrorism, including anti-fraud, anti-corruption and anti-bribery. We have robust and effective risk assessment and due diligence measures and controls in place to ensure compliance with applicable regulations, laws, and standards and ensure continued monitoring and training practice.

We understand that money laundering regulations and legislation place a responsibility on the Company and its employees to combat money laundering across a broad spectrum, including financial transactions, including the possession or dealing in any way or concealment of the proceeds of any crime. We operate in a transparent environment with assessment, tracking, and reporting at the core of our compliance functions. We are dedicated to the prevention of financial crime and continue to improve existing measures.

Money laundering regulations and legislation apply to the following entities and individuals:

- Credit institutions
- Financial institutions·
- Auditors, outside accountants and tax advisers, and any other person who undertakes to provide, directly or through other persons with whom that other person is related, material aid, assistance or advice in tax matters as a principal business or professional activity
- notaries and other independent legal professionals, when they are involved, either acting on behalf of and for their client in any financial or real estate transaction, or assisting in the planning or execution of transactions for their client in relation to:
    - Buying and selling real estate or business entities
    - Management of Clients' Money, Securities, or Other Assets

- Opening or managing bank, savings or securities accounts
- Organization of the contributions necessary for the creation, operation or management of companies
- Creation, operation or administration of trusts, companies, foundations or similar structures.

- Fiduciary or business service providers.
- Real estate agents and rental agents.
- other persons who trade in goods to the extent that payments are made or received in cash in an amount equal to or greater than USD 10,000, whether the transaction is made in a single transaction or in several transactions that appear to be linked.
- Casinos and gambling service providers.
- Providers dedicated to exchange services between virtual currencies and fiat currencies.
- Custodial wallet providers.
- persons who trade in or act as intermediaries in the trade in works of art, including when carried out by art galleries and auction houses, where the value of the transaction or a series of related transactions amounts to USD 10,000 or more.
- persons who store, trade or act as intermediaries in the trade in works of art, when this is carried out through free ports, when the value of the transaction or of a series of related transactions amounts to USD 10 000 or more.

2 PURPOSE

The purpose of this policy is to ensure that the Company complies with the obligations and requirements set forth by Canadian legislation, regulations and standards with respect to the prevention, identification and reporting of money laundering or terrorist financing. This includes ensuring adequate systems and controls

to mitigate risks posed to customers.

This policy provides guidance and a systematic approach for our employees to ensure that their knowledge and understanding of financial crime regulations is exemplary and sets out our expectations and their responsibilities under the regulations as well as the Company's objectives. We provide a comprehensive and effective training program focused on money laundering regulations and the associated requirements of government bodies, and we conduct regular reviews and monitoring to assess and evidence employees' understanding and application of those requirements.

The Company takes all reasonable steps to protect both employees and customers from exposure to money laundering and terrorist financing. Our prevention controls are derived from a risk-based, enterprise-wide approach to identifying, reducing, and mitigating financial crime. Actual or suspected acts of money laundering are reported to FINTRAC and, where appropriate, to the relevant supervisory authority.

3 SCOPE

This policy applies to all Company personnel (i.e., permanent, fixed-term, and temporary staff, third-party representatives or subcontractors, agency workers, volunteers, interns, and agents hired by the Company in Canada or abroad). Compliance with this policy is mandatory and failure to comply could result in disciplinary action.

4 WHAT IS FINANCIAL CRIME AND MONEY LAUNDERING?

Financial crimes are any type of criminal conduct related to money, securities, reduction of liability, tangible or intangible goods and/or financial services or markets. This includes any crime that involves:

- Fraud or dishonesty; or misconduct or misuse of information related to a financial market; or handling of proceeds of crime; or the financing of terrorism.

- The Company aims to identify, mitigate, and prevent financial crimes within its services and activities by implementing policies and procedures that identify, assess, monitor, and manage money laundering and any other associated risks.

- Money laundering is the term used to describe the process or act of disguising or concealing the original ownership of money that has been obtained through criminal acts such as terrorism, corruption, or fraud. Such money is moved through legitimate companies or sources to make it appear "clean."

4.1 Relevant Laws and Regulations

Canada has numerous laws and regulations governing money laundering and terrorist financing. **These include:**

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

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR).

- Criminal Code of Canada.

- Financial Reporting and Transaction Analysis Centre of Canada (FINTRAC).

- Superintendence of Financial Institutions (OSFI).

- Canadian Anti-Money Laundering and Countering the Financing of Terrorism (AML/AFT) Regime.

Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA): This is Canada's main legislation relating to anti-money laundering (AML) and countering the financing of terrorism (CTF) measures. It sets reporting requirements for various entities, including financial institutions, casinos, real estate brokers, and others. It also outlines the obligations of customer due diligence, record keeping, and reporting of suspicious transactions.

Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR)

This regulation provides specific requirements and guidance for the implementation of the PCMLTFA. They detail the procedures and measures that reporting entities must follow to comply with their obligations under the Act.

Criminal Code of Canada: Several provisions of the Criminal Code address money laundering and related offences, providing legal mechanisms to prosecute individuals and entities involved in money laundering activities.

Financial Reporting and Transaction Analysis Centre of Canada (FINTRAC): FINTRAC is Canada's financial intelligence unit responsible for collecting, analyzing, and disseminating financial intelligence related to money laundering, terrorist financing, and other threats to the integrity of Canada's financial system. It operates within the framework of the PCMLTFA and the PCMLTFR.

Office of the Superintendent of Financial Institutions (OSFI): OSFI oversees federally regulated financial institutions in Canada, ensuring their compliance with AML and CTF requirements. OSFI issues guidelines and advisories to help institutions implement effective AML and CTF programs.

Canadian Anti-Money Laundering and Countering the Financing of Terrorism (AML/ATF) Regime: This regime encompasses various guidelines, advisories, and best practices developed by regulatory authorities, industry associations, and government agencies to enhance Canada's AML and CTF efforts.

1 SUPERVISION

Any organisation to which the Money Laundering Regulation applies must be supervised by a supervisory authority. Those companies that are already authorized by the Financial Reporting and Transaction Analysis Centre of Canada (FINTRAC). The company's Supervisory Authority is **FINTRAC.**

1.1 THE FINANCIAL ACTION TASK FORCE (FATF)

The FATF is the global anti-money laundering and terrorist financing watchdog, of which Canada has been a member since 1990. They set international standards with the aim of preventing illegal activities and the harm they cause to society. The FATF is a policy-making body and works with governments to improve or introduce national legislative and regulatory reforms in anti-money laundering controls. As a member of the FATF, Canada works with other member countries to develop and implement effective measures to combat money laundering and terrorist financing globally.

The Company uses the FATF Recommendations and Standards as a resource to ensure effective and compliant AML controls and measures. We also use the FATF list of high-risk countries when considering due diligence.

1 RESPONSIBLE PERSONS OR REPORTING OFFICERS

Depending on the industry in which an organization works, they may have multiple reporting officer obligations and/or be required to pass FINTRAC's a proper and appropriate assessment before registering.

1.1 MONEY LAUNDERING REPORTING OFFICER

Many of the sectors to which the Money Laundering Regulation applies are also regulated by FINTRAC, so there are additional requirements including the appointment of an 'Official Reporting Money Laundering (MLRO)'.

The MLRO is responsible for overseeing the Company's compliance with FINTRAC's rules on systems and controls to prevent money laundering. The organization must ensure that its MLRO has a sufficient level of authority and independence within the Company to enable it to perform its role and that it has access to sufficient resources and information to enable it to carry out its obligations.

When an organization is required to appoint both a Money Laundering Reporting Officer and an MLRO, the same employee may perform both functions. Where the Company has appointed an MLRO; in addition to the obligations of the Money Laundering Reporting Officer, they are also responsible for:

- Oversight of the operation of the Company's anti-money laundering policies and procedures.
- Respond promptly to any reasonable request for information made by FINTRAC.

2 OBJECTIVES

To prevent financial crime and money laundering within our organization, the Company aims to meet the following objectives:-

- Establish and maintain policies, controls, and procedures to effectively mitigate and manage money laundering and terrorist financing risks.
- Notification and detection of suspected money laundering to FINTRAC.
- All staff are trained and should remain vigilant for signs of money laundering.
- All staff follow due diligence and customer identification procedures.
- Maintain strict controls and procedures to detect and report any suspicious activity.
- Frequent risk assessments and audits of all anti-money laundering and countering the financing of terrorism controls and systems.
- To appoint a Money Laundering Reporting Officer with sufficient knowledge and seniority to carry out the tasks and objectives set forth herein.
- Review and maintain customer verification and due diligence procedures.
- Implement procedures that allow the reporting of suspicions of money laundering.
- Maintain record-keeping procedures.
- Use an employee screening program to ensure due diligence.
- Comply with laws, legislation, regulations and supervisory authority guidelines to prevent financial crime, terrorist financing and money laundering.

3 PROCEDURES AND CONTROLS

Money Laundering Regulations and those that oversee the prevention of financial crimes require all companies to have robust and dedicated policies, procedures, and controls in place to assess risk and combat money laundering. **These controls include:**

- Risk assessment.
- Customer due diligence.
- Monitoring, management and internal communication of policies and controls.
- Record keeping.
- Staff awareness and training.
- Report suspicious activity.
- Compliance management.
- Reporting procedures.

3.1 INTERNAL CONTROLS AND MEASURES

In the risk assessment and prevention of money laundering and terrorist financing, the Company has developed and implemented internal controls and measures designed to identify and mitigate risks. These controls comply with money laundering regulations and are reviewed annually to ensure suitability, effectiveness and compliance.

The Company:

- It has established and maintains policies, controls, and procedures for the purpose of preventing money laundering and terrorist financing within the organization.
- Regularly reviews and updates anti-money laundering policies, controls, and

procedures and those associated with our anti-money laundering program.

- A person who has been appointed is a member of the Board of Directors as the officer responsible for AML compliance. The officer(s) are named in this policy and their role has been disseminated against all employees and agents.

- Has, using risk management policies and procedures; Effectively identified, assessed, and managed risks associated with the use or exploitation for financial crime.

- It ensures that adequate resources and funds are made available to address the risk of money laundering and terrorist financing.

- Conduct a thorough selection of employees and agents. It has established an independent audit function that:

    - It examines and assesses the adequacy and effectiveness of the policies, controls and procedures adopted by us for the prevention of money laundering and financial crime.

    - produces management information and gap analysis reports, providing improvement measures and action plans associated with the MLRO and directors.

    - Effectively follow up on such action plans to ensure the finalization and implementation of recommendations.

    - It has implemented an extensive training program for new employees and existing staff regarding money laundering and financial crime prevention, risk assessment, and internal controls.

- After we have appointed a Money Laundering Reporting Officer and, where appropriate, we have notified the relevant supervisory authority of your identity and the appointment.

- It has established customer identification procedures, with customer verification checks and due diligence being performed on all new and existing customers. The

Company never forms a relationship with clients who have not been verified through our strict due diligence measures.

- Use the due diligence questionnaires that act as an application form for new customers, suppliers, employees, and other relevant third parties and ask detailed questions about the company

- Obtained verification and evidence of customers, suppliers, and employees through due diligence checks and obtained supporting documents (if applicable).

- Evidence traceable transactions by ensuring that all transactions made by the Company are recorded in such a way that their origin can be traced should the need arise.

- When requested by our supervisory authority, it has designated a person to act as a central point of contact in Canada for the supervisory authority in any matter relating to the prevention of money laundering or terrorism.

3.2 PROLIFERATION FINANCING

The definition of proliferation financing in the Regulation is "the act of providing funds or financial services for use, in whole or in part, in the manufacture, acquisition, development, export, transshipment, brokering, transport, transfer, stockpiling or any other type of connection with the possession or use of chemical, biological, radiological or nuclear weapons, including the provision of funds or financial services in relation to the delivery systems of such weapons and other CBRN-related goods and technology, in contravention of a relevant financial sanctions obligation.'

In accordance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA),** the Company recognizes its obligation to take appropriate steps to identify and assess proliferation financing risks related to our business type and sector. Our existing risk assessment tools have been updated to include the relevant criteria for assessing such risks. We have also updated these policies and related policies to include controls for identifying, mitigating and managing risks associated with proliferation financing.

The Company uses data obtained from AML risk assessments and due diligence to identify, qualify and manage risks associated with proliferation financing.

3.3 RISK ASSESSMENT

Relevant individuals should complete a business-wide risk assessment to assess the money laundering, terrorist financing and proliferation financing risks to which their business is subject. The Company operates a risk-based approach to these risks and uses risk assessments, tools, and controls to mitigate and manage such risks.

Our risk-based approach involves:

- Identify money laundering risks that are relevant to our business.
- Record these risks in our risk register.
- Conduct detailed risk assessments in the risk areas detailed below.
- Develop controls and procedures to directly manage and reduce the impact of identified risks.
- Monitoring controls and improving their efficiency.
- Maintain records of all risk assessments, reviews, and improvement action plans.

When assessing the risks of money laundering and terrorist financing, we consider:

- The types of customers we have.
- Where those customers are located (i.e., FATF high-risk countries, Canada's list of high-risk countries).
- Types of transactions and volumes.
- Products and services offered and/or activities carried out.
- Channels for individuals/companies to become customers.

- Reliance on and/or use by third parties.
- Tracking customer behavior.
- Product/service delivery channels.
- Payment processing (i.e. cash, transfers (electronic or bank), etc.).
- How funds are allocated, accepted, and maintained.
- Internal and external risks (i.e. customers, outsourcing, markets, systems, etc.).

In accordance with the supervisory authority's requirements on the prevention of money laundering and financial crime, we operate a risk-based system that is fully documented and ensures that 'source of funds' checks and additional verification are obtained on payments under $10,000 when:

- The customer has submitted cash in payment for the transaction, which is five times the size of an average transaction for their business.
- The customer has paid for the transaction by check or debit card, which is ten times the size of an average transaction.

3.3.1 AML Risk Assessment

The Company uses a written risk assessment template to identify, assess, and monitor all risks associated with money laundering and terrorist financing. A review is

It is completed **monthly,** and all risks are reassessed, and any new risks are included in the review.

The Company acknowledges its obligation to take appropriate steps to identify and assess the money laundering and terrorist financing risks to which the Company is subject and to maintain an up-to-date written record of all actions we have taken in the risk assessment process. We understand our obligation to provide the completed risk assessment and any supporting materials and information to our supervisory

authority upon request.

3.3.2 TAX EVASION

The Company has obligations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) to prevent tax evasion through its services and business activities. The Company conducts a **monthly** company-wide money laundering risk assessment that includes identifying risk factors for tax evasion. The Company adheres to a Tax Evasion Policy to follow the rules set forth in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.

The guidance published in conjunction with the PCMLTFA sets out the controls and processes that the Company can implement to help limit the risk of facilitating tax evasion. **These are based on 6 guiding principles:**

- Risk assessment.
- Proportionality of risk-based prevention procedures.
- High-level commitment.
- Due diligence.
- Communication and training.
- Follow-up and review.

3.4 DUE DILIGENCE

The Company adheres to and complies with the Know Your Customer principles, which aim to prevent financial crime and money laundering through customer identification and due diligence. We take a risk-based approach and conduct strict due diligence checks and continuous monitoring of all clients, clients and transactions.

In accordance with money laundering regulations, we use 3 levels of due diligence checks, depending on risk, transactions, and client.

- **SDD: Simplified** due diligence is used in extremely low-risk cases, possibly for existing customer checks or those with low, one-time transactions.
- **DDC: Customer** due diligence is the standard for due diligence checks used in most cases for verification and identification.
- **EDD:** Enhanced due diligence is used for high-risk clients, large transactions or specialized instances such as PEPs or those from FATF high-risk countries or included in Canada's Money Laundering and Terrorist Financing List. (Amendment) (High-Risk Countries) of 2021.

In accordance with the Joint Money Laundering Steering Group (JMLSG), we adhere to the following basic obligations with respect to due diligence:

- You must carry out the prescribed CDD measures for all customers who are not covered by the exemptions.
- They must have systems in place to deal with identification problems in relation to those who are unable to present the standard tests.
- It should apply enhanced due diligence to take into account the increased potential for money laundering in cases of increased risk, especially when the customer is not physically present at the time of identification, and with respect to PEPs and correspondent banking.
- Some persons/entities should not be treated.
- It must have specific policies in relation to the financial (and socially) excluded situation.
- If satisfactory proof of identity is not obtained, the business relationship should not continue.

- You must have some system in place to keep customer information up to date.

3.4.1 STANDARD DUE DILIGENCE ASSESSMENT

For those people or companies considered low risk; We conduct standard due diligence checks, including background and identification checks conducted prior to continuing the business relationship.

The Company recognizes that due diligence checks are mandatory in Canada when:-

- Establish a business relationship.
- Making an occasional transaction that amounts to a transfer of funds in excess of $1,000.
- Suspicion of money laundering or terrorist financing.
- doubt the veracity or suitability of documents or information previously obtained for identification or verification purposes.

The Company also acknowledges the requirement to apply customer due diligence measures when we carry out an occasional transaction amounting to 15,000 USD or more, whether the transaction is executed on a single transaction or on multiple transactions that appear to be linked (excluding rental agents; high-value merchants; art market participants; a crypto-asset exchange provider or a casino).

Where we operate as a **financial services provider,** we will apply customer due diligence measures if we make an occasional cash transaction amounting to $10,000 or more, whether the transaction is executed in a single transaction or in multiple transactions that appear to be linked.

In addition to our standard due diligence measures for new business relationships. **We also carry out standard due diligence measures:**

- where we have a legal obligation during the calendar year to contact an existing customer for the purpose of reviewing any information that:

- is relevant to the Company's risk assessment for that client, and refers to the client's beneficial ownership, including information that enables the Company to understand the ownership or control structure of a legal person, trust, foundation or similar arrangement that is the client's ultimate beneficiary.

- When the Company must contact an existing customer.
- At other times appropriate for existing clients in a risk-based approach.
- When the Company realizes that an existing client's circumstances relevant to its risk assessment for that client have changed.

The Company ensures that, through our due diligence questionnaire and KYC processes, we:

- Identify the customer and verify such identity, (unless that customer's identity and verification is known and has already been verified by the Company).
- Evaluate and, where appropriate, obtain information on the purpose and intended nature of the business relationship or occasional transaction.

When the business relationship involves a legal entity, the Company takes steps to understand the ownership and control structure of the entity and ensures that such information is verified. The Company also obtains records through its due diligence questionnaire and onboarding process:

- The name of the legal entity.
- The company number or other registration number.
- The address of the registered office and, if different, the principal registered office.

The Company takes all reasonable steps to determine and verify the law to which the legal entity is subject and its incorporation, as well as the full names of the board of directors and the high-level persons responsible for the operations of the legal entity.

The Company uses a Due Diligence Policy, a Checklist and a Questionnaire to obtain and record relevant verifications, information and background searches; all of which are kept for a period of 5 years after the end of the business relationship.

1.1.1 ENHANCED DUE DILIGENCE ASSESSMENT

For those individuals or companies assessed as medium to high risk, the Company conducts additional due diligence checks in addition to standard searches and checks. This enhanced due diligence includes checks on financial and criminal background, references, source of funds/wealth, business partners, activities, information about the owner and/or business relationship, and enhanced identity verification.

The Company investigates the reason for any transaction, the purpose of the business relationship, and continuously monitors the client and the business relationship at regular intervals. Enhanced due diligence questions are detailed in our standard due diligence questionnaires, but are only completed when the need for EDD or high-risk customers has been identified.

In accordance with the Money Laundering Regulations, the Company applies enhanced customer due diligence measures and enhanced continuous monitoring (in addition to our standard due diligence measures):

- When the risk of a natural or legal person has been assessed and classified as having a higher risk in terms of money laundering or terrorist financing.
- Where any document or due diligence response obtained is inconclusive to prove an identity or a registered/residential address.
- When the customer has not been physically present for identification purposes or, in the case of legal persons, when a physical visit to the site has not been made.
- When the natural or legal person is from outside Canada.
- When the client or potential client is a PEP, or a family member or a known close associate of a PEP.

- In any business relationship with a person established in a high-risk third country or in relation to any relevant transaction where any of the parties to the transaction is established in a high-risk third country.
- In relation to correspondent relations with a credit institution or a financial institution.
- When a client has provided false identification documentation or information, and the Company proposes to continue dealing with that client.
- In any case, where:
    - A transaction is complex and unusually large, there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose.
- In any other case that by its nature may present a greater risk of money laundering or terrorist financing.

Those we evaluate require EDD are flagged and monitored every **two weeks** and we conduct due diligence checks and reevaluations quarterly instead of our usual annual checks. Additional background checks are conducted on financial status, business history, criminal checks, and status, and enhanced assessments are performed that are not covered by our standard customer due diligence.

Such additional due diligence may include (but is not limited to):

- Obtain information about the client and, where appropriate, the beneficial owners.
- Obtaining the source of funds/wealth.
- Additional information about an individual, position, or employment.
- Due diligence on known family members and close associates.
- Geographical implications.
- Transaction history.

- Enhanced references and additional information on previous, existing, and planned business relationships.
- Obtaining information about the reasons for transactions.
- Obtain approval from senior management to establish or continue the business relationship.
- Conduct improved monitoring of the business relationship by increasing the number and timing of controls applied and selecting transaction patterns that need closer scrutiny.

1.1.2 MONITORING AND AUDIT DUE DILIGENCE

The **MLRO** company is responsible for ensuring that due diligence checks and anti-money laundering measures are completed and fit for purpose. Monthly audits are completed on due diligence forms, company verifications, and customer identity checks to ensure that staff are carrying out due diligence and AML processes in accordance with this policy and any regulatory requirements.

We also carry out **semi-annual checks of** all ID and background searches and archived documents to ensure they remain relevant, appropriate and up-to-date.

1.1.3 VERIFICATION

According to the Money Laundering Regulations, when the Company uses the term "verify", it refers to verification based on documents and/or information obtained from a reliable source that is independent of the person whose identity is being verified.

Documents issued or made available by an official body shall be considered independent even if they are provided or made available to the person concerned by or on behalf of that person. Documents and/or information are considered to originate from a reliable source independent of the person whose identity is being verified when:

- It is obtained through an electronic identification process, including through the use of

electronic identification means or through the use of a trusted service; and

- That process is safe from fraud and misuse and is capable of providing assurances that the person claiming a particular identity.

- It is in fact the person with that identity, to the extent necessary to effectively manage and mitigate any risk of money laundering and terrorist financing.

1.2 Electronic Money and Cryptocurrencies

The Financial Reporting and Transaction Analysis Centre of Canada (FINTRAC) provides stronger oversight and controls when transactions and/or services involve the use of money or digital assets. **In accordance with the latest money laundering regulations, we define:-**

- **'Electronic money'** is electronically (including magnetically), stored monetary value, represented by a right in the issuer that is issued upon receipt of funds for the purpose of performing payment transactions (excluding stored monetary value and monetary value that is used to perform payment transactions.

- **'Virtual currencies'** as a digital representation of value that is not issued or guaranteed by a central bank or an authority, that is not necessarily attached to a legally established currency and that does not possess a legal status of currency or money, but that is accepted by natural or legal persons as a medium of exchange and that can be transferred, stored and marketed electronically.

- **'Custodial Wallet Provider'** As an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.

- **'Acquire'** As a payment service provider that contracts with a payee to accept and process card payment transactions, which result in a transfer of funds to the payee

As the Company uses a form of electronic money as part of its products/services, we recognise that, where a proper risk assessment demonstrates

a low risk, we are exempt from certain customer due diligence measures with respect to electronic money.

We ensure that we keep sufficient track of our business relationship with e-money users and transactions made using the relevant payment instrument to enable us to detect any unusual or suspicious transactions.

1.3 HIGH-RISK IDENTIFICATION

When an individual is classified as high-risk, we conduct enhanced due diligence checks (see the Due Diligence Policy for more information) and ensure that they are marked as part of a high-risk category.

We consider high risk to be:

- Politically exposed people.
- Family members and/or close friends of the PEP's.
- Final Beneficiaries.
- High net worth individual(s).
- Customers with large and/or complex transactions
- Unusual transactions or patterns.
- Entities registered in Countries classified as High Risk by the FATF or the Money Laundering and Terrorist Financing (Amendment) (High Risk Countries) Regulations 2021.
- Unregistered organizations.

When assessing whether there is a high risk of money laundering or terrorist financing in a particular situation, the Company conducts an AML risk assessment to make informed decisions about the scope of measures that need to be taken to manage and mitigate that risk. The risk factors we consider are detailed in the

aforementioned evaluation.

1.3.1 HIGH-RISK COUNTRIES

The Company regularly refers to the FATF's list of high-risk countries and other supervised jurisdictions and ensures that enhanced analysis and due diligence are conducted. Canada no longer refers to high-risk countries as identified by the Canadian Government. Instead, it has published a Statutory Notice that came into force on March 26, 2021.

The Money Laundering and Terrorist Financing (Amendment) (High-Risk Countries) Regulations 2021 is referred to in MLR17 under the obligation to apply the enhanced customer due diligence section and denotes a high-risk third country such as those specified in Annex 3ZA of the instrument.

Canada's current list of high-risk third countries is as follows:

- Albania.
- Barbados.
- Botsu.
- Burkina Faso.
- Cambodia.
- Cayman Islands.
- Democratic People's Republic of Korea.
- Ghana Iran.
- Jamaica.
- Morocco.

- Myanmar.
- Nicaragua.
- Pakistan.
- Panama.
- Senegal.
- Syria.
- Uganda.
- Yemen.
- Zimbabwe.

1.1.1 POLITICALLY EXPOSED PERSONS (PEPS)

A Politically Exposed Person (PEP) is a person who has been or has been entrusted with a prominent function and, as such, could abuse such position or function for the purposes of money laundering or other associated crimes, such as corruption or bribery. Due to the high risks associated with PEPs, the Action Group.

Financiera Internacional (FATF) recommends that additional AML and due diligence controls and measures be put in place when entering into a business relationship with a PEP.

The Company utilizes existing business resources and other databases for PEP identification and verification and always ensures that initial due diligence KYC checks include reviewing individual names with those resources and databases to identify PEPs immediately. We also maintain our own internal PEP list against which to cross-check KYC data.

The Company uses additional due diligence measures for all identified Politically Exposed Persons (PEPs) and, where there is such a proposal to establish a business relationship or carry out a one-time transaction with a PEP, **we always ensure that:**

- The approval of the director or Senior Management to establish the business relationship is obtained and recorded.
- We take reasonable steps to establish the source of wealth and the source of funds.
- We carry out continuous monitoring of the business relationship.

1.1.2 Beneficial Owners

The Company uses the Central Register and our own verification checks to identify and register Beneficial Owners**. Under** the Money Laundering Regulations**,** Canada is required to create and maintain a directory of beneficial owners of corporate entities incorporated in Canada, allowing for additional due diligence measures to verify what clients have told us about their ownership.

We consider beneficial owners to be higher risk and as such, we conduct increased due diligence when developing a new business relationship. **We seek to obtain and register:**

- Names of the final beneficiaries.
- Dates of birth.
- Nationality.
- Nature and description of the real ownership.
- If the beneficial owner is a legal person, trust, company, foundation or similar legal arrangement and take reasonable steps to understand the ownership and control structure of that legal person, trust, company, foundation or similar legal arrangement.

We use individual and business Due Diligence Questionnaires to retain written records of the actions the Company takes to identify the ultimate beneficiary of the corporation and to verify the identity of the senior person in the corporation responsible for managing it (including any additional information or difficulties in obtaining the required details).

Please refer to our **due diligence program** for further guidance on our verification measures and acceptable proof and identity documents.

1.1.1 THIRD-PARTY TRUST

The Company understands that it may rely on a third party to implement relevant customer due diligence measures. The Company acknowledges that trust is only valid when the third party is:

- Other relevant person who is subject to the Money Laundering Regulations.
- A person carrying on a business activity in a third country who:
    - Subject to requirements in relation to customer due diligence and record-keeping equivalent to those set out in the Money Laundering Regulation; and monitored compliance with those requirements
- organizations whose members consist of individuals within the two preceding paragraphs.

The Company understands that it remains liable for any failure to conduct or verify adequate due diligence measures. Therefore, we have controls and tools in place to help us agree, verify, and monitor any trusted relationships with third parties that we have. The following documents complement our existing due diligence policy and controls where reliance on due diligence is a factor:

- Third Party Trust Agreement.
- Third-party trust questionnaire (for natural and legal persons).
- Third-party trust registration.
- Letter of request of trust from third parties.

The above documents enable us to use an agreement for any reliance on a third party and to ensure that adequate and compliant due diligence checks have been carried out and that we have an accurate record of them. When the Company relies on a third party to apply due diligence measures to the client, we:-

- Always have an agreement before accepting information from a third party.
- Use a record to record who the third parties we use are and why we rely on them.
- Use a standardized request letter template when requesting and obtain the relevant due diligence information from the third party.

- Obtain immediately from the third party all information necessary to comply with the requirements of the Regulation, in particular:
    - Identify the customer and verify their identity.
    - Evaluate and obtain information about the purpose and intended nature of the business relationship or occasional transaction.
- Where the customer is a legal entity, obtain and verify:
    - the name of the legal entity and its company number or other registration number.
    - the address of its registered office and its main place of business.
    - the law to which the legal entity is subject and the full names of the board of directors, the superior persons and/or the administrative body.
- Where the customer is a legal person, trust, company, foundation or similar legal arrangement, please take reasonable steps to understand the ownership and control structure of that entity or arrangement.
- Where the customer is the beneficial ownership of another person:
    - Identify the beneficial owner and take reasonable steps to verify the identity of the beneficial owner.
    - Where appropriate, take reasonable steps to understand the ownership and control structure of the entity or a similar legal instrument.
- Where an institution acts on behalf of the customer:
    - Verify that the entity is authorized to act on behalf of the customer.
    - Identify the entity and verify its identity on the basis of

documents or information obtained from a reliable source, which is independent of the entity and the client.

- Collect an extract from the register containing all the details of the beneficial owners (or registrable beneficial owners in relation to a foreign entity).

- Have an agreement in place with the third party ensuring that we can obtain, upon request, copies of any identification and verification data and any other relevant documentation regarding the identity of the customer, the customer's ultimate beneficiary, or anyone acting on behalf of the customer.

1.2 TRANSACTION MONITORING

Money service businesses (MSBs) in Canada have several responsibilities regarding transaction reporting, which are regulated by law. Some of the main responsibilities of MSBs in Canada include:

1. **FINTRAC Registration**: MSBs must register with the Financial Reporting and Transaction Analysis Centre of Canada (FINTRAC) before they begin trading.

2. **Suspicious Transaction** Reporting: MSBs are required to report to FINTRAC any suspicious transactions related to money laundering or terrorist financing.

3. **Reporting Large Cash Transactions**: MSBs must report to FINTRAC any cash transaction of $10,000 CAD or more, whether in a single transaction or in multiple transactions that appear to be related.

4. **Record keeping**: MSBs are required to keep detailed records of all financial transactions, including customer identities and transaction details, for a specified period of time, as required by regulations.

It is important for MSBs to meet these responsibilities in order to comply with regulations and contribute to the prevention and detection of money laundering and terrorist financing in Canada.

2 RECORDS MANAGEMENT

All documents, accounts, and transactions associated with clients are retained based on legal or statutory retention periods, which are currently at Account **Closure + 5 years.** The details of the following records are retained:

- Identification and verification registration.
- Due diligence checks.
- Company incorporation documents (if applicable).
- Transaction lists.
- Audit and review trails.
- Staff training files and evaluation records.

3 REPORTS

Our **MLRO** is responsible for monitoring all anti-money laundering measures and increasing FINTRAC when necessary. In the absence of a designated official, the Deputy Money-Laundering Reporting Officer will be appointed to this function and will have the same responsibilities.

All documents related to money laundering reports, business transactions, customer identification, and customer due diligence are retained for a minimum of 5 years.

The designee shall ensure that the following minimums are met with respect to the information disclosed in any report:

- Full details of the people involved.
- Full details of the nature of your participation.
- The types of money laundering activity involved.
- The dates of these activities.
- Have transactions been made, are they in progress or imminent?

- Where they took place.
- How were they carried out?
- The approximate and/or exact amount of money/assets involved?
- What has given rise to suspicions?
- Using all information available at the time, the NO/MLRO makes an informed decision using sound judgement as to whether there are reasonable grounds for knowledge or suspicion of money laundering and to enable them to prepare their report to the National Crime Agency (FINTRAC), where appropriate.

4 DUE DILIGENCE AND ONGOING AUDITS

The **Compliance Team** is responsible for ongoing due diligence checks over the lifetime of the client's/client's account, ensuring that all information is kept up to date and that no adverse information has emerged since the last follow-up check was carried out. These checks will be carried out on all existing active customers on a continuous annual basis.

The Company uses an Anti-Money Laundering Audit Checklist to audit and review our existing processes, controls, and measures on an ongoing and frequent basis. Audits are conducted quarterly and actions and recommendations for improvement are provided to the Senior Management Team and the **MLRO.**

The Company uses a Compliance Audit and Monitoring Program to review and evaluate all measures, procedures and controls across the business to ensure efficiency, effectiveness and compliance with relevant laws and regulations.

5 TRAINING

The Company has implemented a comprehensive anti-money laundering and financial crime training program to ensure that all personnel responsible for processing transactions and/or initiating and/or establishing business relationships, receive training in AML knowledge, competencies, and awareness. We understand that any company that fails to provide training to its relevant employees could be in breach of regulations and therefore at risk of prosecution.

Our AML training program consists of:

- Training Workshops.
- Evaluation tests.
- 1-2-1 Coaching and Mentoring.
- AML scripts and reminders.
- Intranet and resource.

Our training methods and sessions are tailored to the company to ensure that staff are aware of the different possible money laundering patterns and techniques that could occur in their day-to-day roles and duties. We have a Training and Development Policy and Procedures detailing the measures taken to ensure staff competence and skill, and we also use unique assessment tests and feedback on training assessment to ensure that all training is understood and delivered effectively.

Our Financial Crimes and AML training program ensures that all employees and agents:

- Confident and competent in risk assessment and prevention of money laundering and financial crimes.
- Know the law and associated regulations related to money laundering and terrorist financing.
- Provide regular and relevant training on how to recognize and deal with transactions and other activities that may be related to money laundering or terrorist financing.
- Receive additional training and support when their role is directly related to meeting any regulatory requirements, or able to contribute to:
    - Identification or mitigation of the risk of money laundering and terrorist financing.

- prevention or detection of money laundering and terrorist financing.

5.1 NOTICE

"Giving notice" is an offense that carries an unlimited fine and up to 5 years in prison. The Company takes steps to ensure that deliberate or accidental notice is not a risk factor and that no client is intentionally or inadvertently informed of any SAR investigation or activity that may make them aware of our or FINTRAC's suspicions.

Steps we take to help reduce the risk of "giving notices" include the following:

- **Employee training and awareness:** Our training sessions dedicated to anti-money laundering and financial crime include details on how to receive notices.
- **Customer-facing staff guidance:** In some situations, a transaction may be delayed or a customer relationship needs to be terminated due to an investigation or SAR. In these cases, the Company understands the importance of not "advising the client as to the cause of the delay/determination". The actions we take include:
  - Add detailed notes to a customer account and/or transaction history to ensure that any staff accessing the data are aware of the situation.
  - Make sure that only one dedicated person or the NO deal with the customer in question.
  - Offer alternative reasons to the customer for any delays/terminations that do not raise their suspicions of the suspicious activity.
  - Restrict access to SAR data or internal investigations to reduce the risk of "giving notices."
- **Report lines:** The company has a defined organizational chart that shows the relevant report lines and makes it clear who the MLROs are. By ensuring that employees refer any suspicions to the right person immediately, we reduce the risk

of oversaturation of suspicion and, by default, the risks of giving notices.

- **Information security:** Protecting and restricting access to referrals, suspicions, delayed accounts, terminated relationships, and submitted SARs is critical to prevent many people from finding out about suspicious activity or the customers involved. We have a robust information security program that restricts employee access, access controls, confidentiality, and non-disclosure measures.

6 DATA PROTECTION

The Company has a **data protection compliance program** in place to ensure that we comply with Canada's GDPR, as adapted by the Data Protection Act 2018, which governs the processing of information relating to individuals. Since the scope of our data protection program is broad, any relationship with the processing of information or the disclosure of such information for the purpose of complying with our money laundering obligations can be found in our Data Protection Policy and supporting documents.

As a summary note, we ensure that all clients and those entering into a business relationship with the Company have access to a clear and compliant privacy notice statement that includes details of our money laundering obligations and how personal data will only be used for the purpose of preventing money laundering and terrorist financing in accordance with the requirements of the Article 13 of Canada's GDPR.

The processing of personal data in accordance with this Regulation is lawful and necessary for the prevention of money laundering or terrorist financing and for the performance of a task carried out in the public interest.

7 RESPONSIBILITIES

Responsible individuals within the organization who are responsible for the prevention of financial crimes and compliance with money laundering rules and regulations are recorded in this policy.

It is the Company's policy to ensure that Senior Management has frequently developed, implemented, acted and monitored the following areas in relation to money laundering and terrorist financing:

- Conduct a risk assessment that identifies where the business is or could be vulnerable to money laundering. (including terrorist financing) and create a written summary risk assessment statement based on the findings and mitigation controls

- Ensure that a risk-based approach is adopted to manage identified risks and allocate resources, funds and personnel to areas deemed to be at greatest risk.

- Keep all anti-money laundering policies, controls and procedures up to date and be part of a regular review programme to ensure that changes, systems, up-to-date laws/regulations and guidance materials are frequently reviewed and monitored to reflect the risks faced by the Company

- Educate and train all employees regarding the risks and prevention of money laundering and provide sufficient resources and funding for such training, with a key focus on employees in due diligence-related roles or high-risk clients

- Develop, implement and monitor systems in relation to customer transactions and for activities involving individuals/companies from high-risk third countries (as identified by Canada, FATF or relevant OFSI financial sanctions).

- Review, approve, and monitor any ongoing business relationships with politically exposed persons (including family members and/or known associates of PEP's)

The Company has designated an **MLRO** when necessary and complies with all Canadian legislation and regulations regarding the prevention and mitigation of money laundering risks. We ensure that all employees have the time, resources, and support necessary to learn, understand, and implement AML processes and regulations, and are expected to be on the lookout for any acts of suspected financial crime.