CASHMERE SOLUTIONS LIMITED

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

(AML/CTF Policy)

CASHMERE SOLUTIONS LIMITED
Company Registration No.: 1000765207
Registered in Ontario, Canada

Effective Date: 23.03.2026
Version: 1.1.
Approved by: Board of Directors
Prepared by: AML & Compliance Officer

Confidentiality Notice

This document contains confidential and proprietary information of CASHMERE SOLUTIONS LIMITED. It is intended solely for internal use and for disclosure to authorized third parties, including regulatory authorities, financial institutions, and partners, where required.

Unauthorized use, distribution, or reproduction of this document, in whole or in part, is strictly prohibited.

- This AML/CTF Compliance Program (the “Program”) applies to all branches, subsidiaries, and operations of CASHMERE SOLUTIONS LIMITED (the “Company”).

- This Program consists of a primary policy document, which establishes the general principles and framework governing the Company’s AML/CTF procedures, as well as supporting annexes and internal documents that set out specific processes, controls, and requirements in detail.

- The implementation of this Program does not limit or replace the obligation to comply with all applicable local, national, and international laws and regulations. Nothing in this Program shall be interpreted as permitting any activity that is prohibited or restricted under applicable legislation.

- The Company maintains full cooperation with competent regulatory authorities, financial intelligence units, and law enforcement agencies in Canada and in other relevant jurisdictions, including in relation to regulatory inquiries, investigations, and reporting obligations.

- The Company further ensures that its AML/CTF framework is aligned with international standards, including FATF recommendations, and meets the expectations of financial institutions and electronic money institutions with which it maintains or intends to establish business relationships.

- This Program shall be formally approved and adopted by the Company’s senior management, including the Board of Directors and the Compliance Officer, and shall be subject to periodic review to ensure its ongoing effectiveness and relevance.

Glossary

For the purposes of this Policy, the following terms shall have the meanings set out below:

AML - Anti-Money Laundering
CDD - Customer Due Diligence
CTF - Counter-Terrorist Financing
ODD - Ongoing Due Diligence
EDD - Enhanced Due Diligence
FATF - Financial Action Task Force
FINTRAC - Financial Transactions and Reports Analysis Centre of Canada
ML - Money Laundering
PEP - Politically Exposed Person
EFT - Electronic Funds Transfer
RBA - Risk-Based Approach
RGS - Reasonable Grounds to Suspect (as defined under applicable Canadian AML legislation)
SoF - Source of Funds
SoW - Source of Wealth
TF - Terrorist Financing
UN - United Nations
VASP - Virtual Asset Service Provider
VC - Virtual Currency
FE - Financial Entity
RE - Reporting Entity

Table of Contents

Introduction

The Company adopts appropriate and proportionate measures aimed at preventing its operations from being used to conceal, manage, invest, or transfer funds or other assets derived from illicit activities, or to give the appearance of legitimacy to such activities.

The Company applies a risk-based approach in the design and implementation of this AML/CTF Program, taking into account the nature, scale, and complexity of its operations, as well as the geographic and customer-related risks associated with its business.

A qualified Compliance Officer has been appointed and is responsible for the effective implementation, oversight, and continuous improvement of the Company's AML/CTF policies and procedures.

The Company further ensures that its AML/CTF framework aligns with internationally recognized standards, including FATF recommendations, and meets the expectations of financial institutions and electronic money institutions (EMIs).

Company's Key AML/CTF Principles

In the course of its business activities, the Company adheres to the following principles:

- to comply with applicable AML/CTF legislation in all jurisdictions in which it operates;
- to implement and maintain a risk-based approach to identifying, assessing, and mitigating ML/TF risks;
- to align its policies and procedures with international standards, including the recommendations of the Financial Action Task Force (FATF);
- to cooperate with FINTRAC and other competent authorities, as well as with regulatory and law enforcement bodies in relevant jurisdictions;
- to ensure effective systems and controls for the prevention, detection, and reporting of suspicious activities;
- to assess and, where necessary, restrict or decline business relationships or transactions that exceed the Company's risk appetite or do not meet its compliance standards;

- to comply with the primary AML/CTF legislation of Canada and other applicable regulatory frameworks.

Company's Compliance Program

The Company has established this AML/CTF Compliance Program to ensure that all identified money laundering and terrorist financing risks are appropriately managed and mitigated.

This includes the implementation of adequate systems, controls, and procedures designed to prevent the misuse of the Company's services for financial crime purposes.

The Program is based on a risk-based approach and is supported by ongoing monitoring, internal controls, and periodic reviews to ensure its effectiveness and alignment with regulatory expectations.

The Program defines the core AML and CTF standards and procedures that must be consistently applied across the Company's operations.

The Company ensures that its Compliance Program supports transparency, auditability, and effective cooperation with financial institutions, including EMIs, as well as regulatory authorities.

Program Framework

The Program is based on applicable AML/CTF laws, regulations, and regulatory guidance issued by competent authorities in Canada.

It is further designed to align with international standards, including the Financial Action Task Force (FATF) recommendations on combating money laundering, terrorist financing, and proliferation financing.

Among other things, this Program:

- forms an integral part of the Company's overall compliance framework and is designed to meet the requirements of its legislative and regulatory environment;
- ensures that the Company is able to detect, assess, and report suspicious activities related to money laundering, fraud, and terrorist financing to the appropriate authorities in a timely manner;
- is based on a risk-based approach, focusing not only on the effectiveness of internal systems and controls, but also on the nature and level of risk associated with the Company's customers, products, services, and geographic exposure;
- is built on a strong foundation of regulatory understanding and is overseen by personnel with sufficient experience, expertise, and authority to promote a culture of compliance across all levels of the organization;
- supports effective cooperation with financial institutions, including banks and electronic money institutions (EMIs), as well as regulatory and supervisory authorities.

Review of the Program

This Program shall be reviewed by the Board of Directors and the Compliance Officer at least every two years.

The Program may be reviewed more frequently where required based on regulatory developments, changes in the Company's risk profile, or operational developments.

The Company shall review and, where necessary, update this Program and its annexes (including the risk assessment and related internal policies) in the following circumstances:

- following the publication of national or international money laundering and terrorist financing risk assessments;
- upon receipt of regulatory guidance, recommendations, or orders from FINTRAC or other competent authorities requiring enhancement of internal procedures;
- upon significant changes in the Company's business model, management structure, products, services, or geographic exposure;
- where deficiencies, gaps, or areas for improvement are identified through internal monitoring, compliance reviews, or audits.

The Company also ensures that periodic reviews assess the effectiveness, adequacy, and proportionality of its AML/CTF controls.

This Program's review shall be formally documented and approved by a resolution signed by the Chief Executive Officer and the Compliance Officer.

Governance Principles

The Company's employees and third-party service providers involved in the Company's activities are required to act in accordance with this Program.

The obligations set out in this Program shall be understood as applicable to all employees of the Company, unless specific responsibilities are expressly assigned to designated roles, including but not limited to the Board of Directors and the Compliance Officer.

All employees shall be made aware of this Program and their respective AML/CTF responsibilities, which shall be proportionate to their roles and functions.

The Company ensures that appropriate reporting lines, escalation procedures, and internal accountability mechanisms are in place.

Where applicable, responsible personnel may be appointed to oversee specific functions or structural units, including the supervision of daily operations and compliance with internal policies and procedures.

The Company ensures segregation of duties and avoidance of conflicts of interest in the execution of AML/CTF-related responsibilities.

The Board of Directors is responsible for the overall management and coordination of the Company's operations, including the allocation of responsibilities across structural units and oversight of their performance.

In addition, the Board of Directors ensures that adequate resources, systems, and controls are in place to support effective AML/CTF compliance.

The Board of Directors may, where appropriate, consult with internal and external experts, including employees, advisors, and service providers, in order to support decision-making and compliance oversight.

Company's Services

The Company operates as a Money Services Business (MSB) in accordance with applicable Canadian legislation.

The Company maintains a documented description of its services (including as set out in internal annexes), which defines, among other things:

- the conditions applicable to the provision of each service;
- the operational flow of services, including the movement of funds and/or virtual assets.

The Company provides its services on a cross-border basis, subject to internal risk assessment and applicable regulatory requirements.

The Company delivers its services through various channels, including its website, electronic communications (such as email), and other digital communication channels, including messaging platforms.

Before introducing new services or making material changes to existing services, the Company conducts a documented risk assessment to identify and mitigate potential ML/TF risks associated with such changes.

Such assessment includes, where relevant, risks related to customer anonymity, use of new technologies, cross-border transactions, and involvement of third-party service providers.

Money Laundering

The term "money laundering" (ML) refers to any act or attempted act to conceal or disguise the origin, nature, location, ownership, or control of money or assets derived from criminal activity.

Money laundering typically involves multiple transactions and may include complex financial structures. The Company recognizes that such activities may occur across jurisdictions and through various financial and digital channels, including virtual assets.

There are three commonly recognized stages of money laundering:

1. Placement - the introduction of proceeds derived from illegal activities into the financial system;
2. Layering - the process of separating illicit proceeds from their origin through complex layers of financial transactions designed to obscure the audit trail and provide anonymity;
3. Integration - the process of reintroducing laundered funds into the legitimate financial system, creating the appearance of lawful origin, often through seemingly legitimate business activities.

The Company remains vigilant to indicators associated with each stage and implements monitoring mechanisms to detect such activities.

Terrorist Financing

The term “terrorist financing” (TF) refers to the provision, collection, or use of funds or other assets, by any means, with the intention or knowledge that they will be used, in full or in part, to carry out terrorist acts or support terrorist organizations.

This definition is aligned with international standards, including the International Convention for the Suppression of the Financing of Terrorism (1999), as well as applicable Canadian legislation.

Terrorist financing may involve funds derived from both legal and illegal sources and may be structured to avoid detection through financial systems.

The Company applies strict controls, including sanctions screening and transaction monitoring, to detect and prevent any involvement in terrorist financing activities.

For further reference, see: https://treaties.un.org/doc/db/terrorism/english-18-11.pdf

Despite the differences in structure and stages, the methods used in terrorist financing may be similar to, and in some cases overlap with, those used in money laundering.

Terrorists and terrorist organizations require financial resources to achieve their objectives. In order to avoid detection, they often seek to obscure or disguise the link between themselves and the origin of the funds.

As a result, terrorist groups may use techniques comparable to money laundering to move, manage, and utilize funds, regardless of whether such funds originate from legal or illegal sources. This enables them to access and use financial resources without attracting the attention of regulatory authorities and law enforcement agencies.

The Company recognizes these risks and applies appropriate monitoring, due diligence, and control measures to detect and prevent activities that may be associated with terrorist financing.

AML/CTF Systems

Primary Legislation Governing AML/CTF in Canada

The Company complies with the requirements set out in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), as well as all applicable regulations and guidance issued by competent Canadian authorities.

In addition, the following legal acts are relevant to the Company's activities (non-exhaustive list):

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (SOR/2002-184);
- Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (SOR/2001-317);
- Criminal Code (R.S.C., 1985, c. C-46);
- Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (SOR/2001-360);
- Guidance issued by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), including directives relating to anti-money laundering, counter-terrorist financing, and the implementation of ministerial directives.

The Company also takes into account internationally recognized standards, including the Financial Action Task Force (FATF) recommendations, and aligns its internal controls with expectations of financial institutions and electronic money institutions (EMIs).

The Company firmly believes that maintaining a strong reputation for integrity, transparency, and compliance, both in its business model and in its internal systems and procedures, is essential to achieving its commercial objectives and fulfilling its corporate responsibilities.

Accordingly, the Company is committed to implementing robust AML/CTF measures and maintaining effective internal controls designed to prevent the misuse of its services for money laundering, terrorist financing, or other financial crime-related purposes.

The Company adheres to both applicable legal requirements and internationally accepted best practices in order to ensure a high standard of compliance across all areas of its operations.

Supervisory Authority

For the purposes of AML/CTF compliance, the Company, as a registered Money Services Business (MSB), is supervised by the following competent authority:

- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC);
- Registration number: 1886008786;
- Address: 234 Laurier Avenue West, 24th Floor, Ottawa, ON K1P 1H7, Canada;
- Phone: +1-866-346-8722;
- Email: communications3@fintrac-canafe.gc.ca.

FINTRAC is responsible for overseeing the Company's compliance with applicable AML/CTF legislation, including the assessment of the effectiveness of its compliance program and the receipt, analysis, and dissemination of financial transaction reports submitted by reporting entities.

In addition, FINTRAC performs supervisory functions in relation to both domestic and international obligations, including the implementation and monitoring of applicable sanctions regimes.

Effective Controls

To ensure the proper implementation of AML/CTF procedures and controls, the Company has established and maintains an effective control framework, which includes:

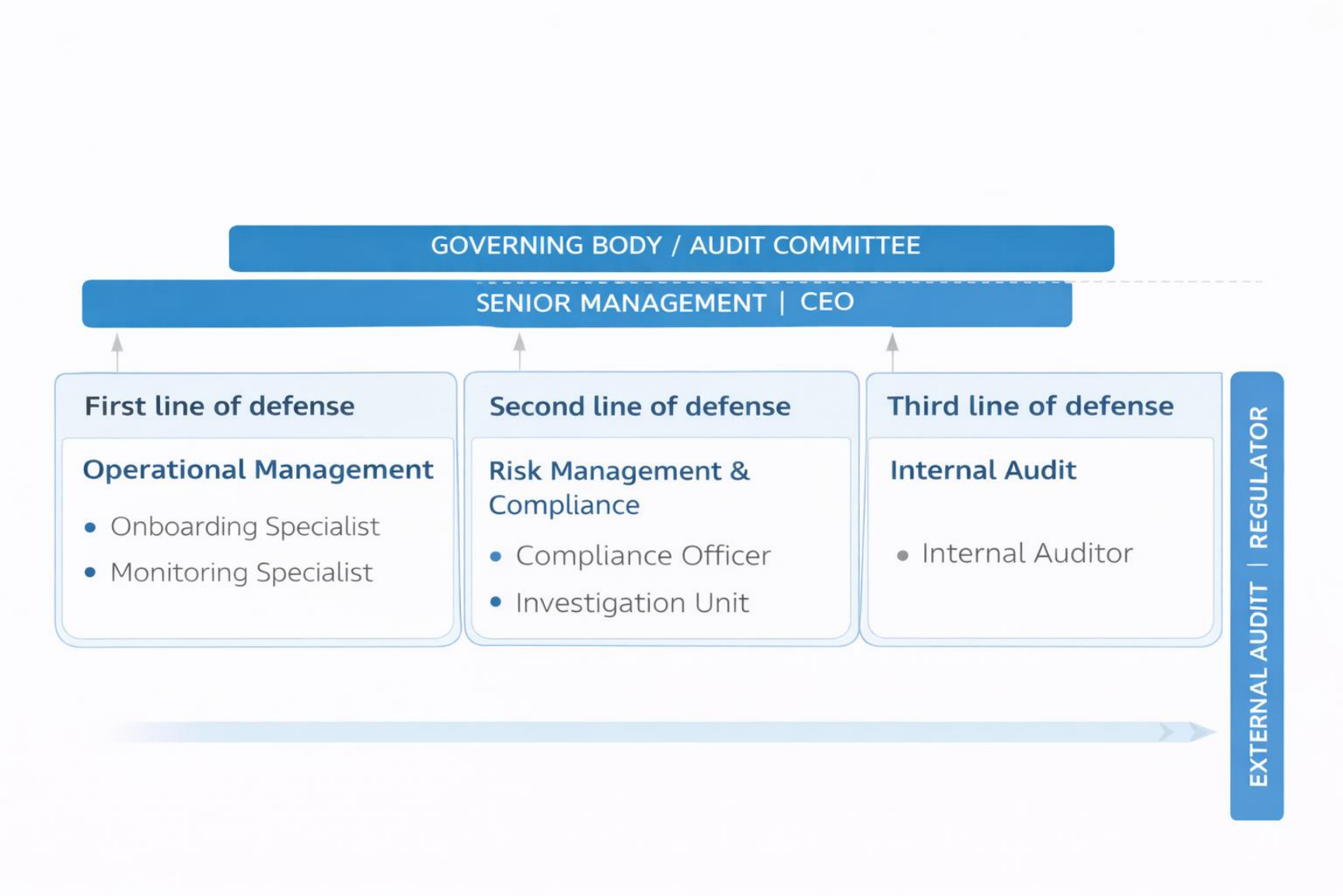
- a comprehensive AML/CTF compliance program;
- active oversight by senior management;
- the appointment of a Compliance Officer and other designated personnel with clearly defined responsibilities;
- independent compliance and review functions, proportionate to the size and nature of the Company's operations;
- ongoing staff training and awareness programs.

The Company ensures that its internal controls are risk-based, proportionate, and regularly assessed for effectiveness.

The Board of Directors is responsible for the overall management of the Company and for ensuring effective oversight of AML/CTF systems and controls.

The Compliance Officer, appointed by the Board of Directors, is responsible for oversight and coordination for the establishment, implementation, and maintenance of the Company's AML/CTF framework and acts as the central point of contact for suspicious transaction reporting and regulatory communication.

The Compliance Officer operates with sufficient independence, authority, and access to resources necessary to perform their duties effectively.


GOVERNING BODY / AUDIT COMMITTEE
SENIOR MANAGEMENT | CEO
First line of defense
Operational Management
Onboarding Specialist
Monitoring Specialist
Second line of defense
Risk Management & Compliance
Compliance Officer
Investigation Unit
Third line of defense
Internal Audit
Internal Auditor
EXTERNAL AUDITT | REGULATOR

Senior Management Responsibilities

The Chief Executive Officer (CEO) and/or Board of Directors are ultimately responsible for the overall management of the Company and for ensuring that effective AML/CTF controls are established, implemented, and maintained.

Senior Management is responsible for overseeing the Company's compliance framework and ensuring that AML/CTF obligations are integrated into all relevant business processes. These responsibilities include, but are not limited to:

- ensuring ongoing compliance with applicable Canadian laws, regulations, and regulatory guidance;
- overseeing and monitoring the Company's compliance activities to ensure alignment with applicable legislation, internal policies, and procedures;
- reviewing the AML/CTF Compliance Program to ensure that it remains comprehensive, effective, and proportionate to the Company's risk profile;
- approving the AML/CTF Compliance Program and any material updates thereto;
- ensuring that the AML/CTF Compliance Program is effectively implemented by the Compliance Officer and relevant personnel;
- appointing a qualified and competent individual as the Company's Compliance Officer;
- regularly assessing the performance and effectiveness of the Compliance Officer;
- ensuring that the Compliance Officer has sufficient independence, authority, and access to adequate resources (including financial, technical, and human resources) to perform their duties effectively;
- reviewing periodic reports submitted by the Compliance Officer and ensuring that identified issues, risks, or deficiencies are appropriately addressed;
- ensuring that the AML/CTF framework supports the integrity, stability, and soundness of the Company's operations;
- reviewing and approving proposed changes to the AML/CTF Compliance Program on a periodic basis;
- ensuring that independent reviews or audits of the AML/CTF framework are conducted, where appropriate, to assess compliance with applicable laws and the effectiveness of internal controls.

Senior Management shall promote a strong culture of compliance across the organization and ensure that AML/CTF considerations are embedded into strategic and operational decision-making.

The Senior Management of the Company has approved this AML/CTF Compliance Program and the appointment of the Compliance Officer, and has delegated responsibility to such officer for the day-to-day management, monitoring, and execution of AML/CTF controls.

At the same time, Senior Management retains ultimate accountability for the effectiveness of the Company's AML/CTF framework.

KYC Agents

KYC Agents constitute the first line of defense within the Company's AML/CTF framework. They are part of the operational risk management system and are responsible for identifying, assessing, and managing ML/TF risks arising from the Company's day-to-day business activities.

The first line of defense plays a critical role in ensuring that risks are identified at the earliest stage and are appropriately escalated where necessary.

KYC Agents are required to maintain a thorough understanding of the Company's customers, including the nature of their business activities, transaction patterns, and risk profiles.

The principal functions of KYC Agents include, but are not limited to:

- conducting customer onboarding procedures, including identification and verification, and applying appropriate Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) measures prior to establishing a business relationship;
- performing ongoing due diligence (ODD), including continuous monitoring of customer activity and periodic review and updating of customer information;
- identifying transactions or patterns of activity that may be considered unusual, suspicious, or inconsistent with the customer's known profile or expected economic purpose;
- escalating suspicious or potentially suspicious activities to the second line of defense (Compliance Department) for further review and, where appropriate, to Senior Management;
- maintaining accurate and complete records of customer information, due diligence measures, and monitoring activities;

- performing other functions as required under applicable laws, internal policies, and job responsibilities.

KYC Agents act as the primary point of control for the detection of ML/TF risks and are expected to exercise professional judgment and vigilance in the performance of their duties.

Compliance Department

Compliance Officer

The Compliance Officer serves as the central point of oversight within the Company for all matters relating to the prevention, detection, and reporting of money laundering and terrorist financing.

The Compliance Officer is responsible for ensuring that the Company's AML/CTF framework is effectively implemented, maintained, and continuously improved, and for providing guidance and support to Senior Management in managing ML/TF risks.

Key responsibilities of the Compliance Officer include:

- overseeing the implementation and effectiveness of AML/CTF policies, procedures, and controls;
- monitoring compliance with applicable laws, regulations, and internal policies;
- reviewing and analyzing escalated cases, including suspicious activities identified by the first line of defense;
- determining whether a transaction or activity meets the threshold for reporting to FINTRAC or other competent authorities;
- ensuring timely and accurate submission of required reports;
- maintaining communication with regulatory authorities and financial institutions, where applicable;
- providing AML/CTF-related advice and training to employees;
- ensuring that appropriate risk assessment and monitoring frameworks are in place and functioning effectively.

The Compliance Officer operates independently from operational functions and has a direct reporting line to Senior Management.

The Compliance Officer is granted sufficient authority, access to information, and adequate resources (including financial, technical, and human resources) necessary to perform their duties effectively.

Additional Responsibilities of the Compliance Officer

In particular, the Compliance Officer is responsible for:

- developing, implementing, and continuously reviewing the Company's AML/CTF systems, including the risk assessment framework, to ensure they remain up to date and aligned with applicable legal and regulatory requirements;
- overseeing all aspects of the AML/CTF framework, including monitoring its effectiveness and ensuring that controls and procedures are enhanced where necessary;

The Compliance Officer plays a central role in ensuring that the Company's AML/CTF systems remain effective, proportionate, and responsive to evolving risks.

The Compliance Officer also plays an active role in the identification, assessment, and reporting of suspicious transactions. Key responsibilities include:

- reviewing all internal disclosures, alerts, and exception reports, and determining whether reporting obligations to FINTRAC or other competent authorities are triggered (including STRs, LCTRs, LVCTRs, and other applicable reports);
- maintaining complete and accurate records of all internal reviews, investigations, and reporting decisions;
- ensuring that appropriate measures are in place to prevent "tipping-off" in accordance with applicable legal requirements;
- acting as the primary point of contact with FINTRAC, law enforcement authorities, and other competent bodies in matters relating to AML/CTF compliance, investigations, and reporting.

In addition, the Compliance Officer:

- oversees the ongoing monitoring of the Company's business relationships and ensures that monitoring activities are performed on a regular and risk-based basis;
- identifies, reviews, and escalates suspicious transactions and activities where necessary;
- monitors regulatory developments and changes in AML/CTF requirements and ensures that relevant updates are communicated to Senior Management and implemented within the Company;

- develops and delivers internal AML/CTF training programs and materials, and ensures that relevant personnel receive adequate and ongoing training;
- acts as the designated responsible person under applicable AML/CTF legislation (including PCMLTFA and related regulations) for the implementation and maintenance of the compliance program;
- performs any additional functions assigned under applicable laws, internal policies, and the Company's governance framework.

The Compliance Officer ensures that all AML/CTF-related activities are properly documented, auditable, and capable of being reviewed by regulatory authorities and financial institution partners.

Investigation Unit

The Investigation Unit operates under the supervision of the Compliance Officer and forms part of the second line of defense within the Company's AML/CTF framework.

The Investigation Unit supports the Compliance Officer in the analysis, assessment, and escalation of potentially suspicious activities and transactions.

Its functions include, but are not limited to:

- assisting the Compliance Officer in reviewing internal disclosures, alerts, and exception reports;
- supporting the preparation and submission of reports to FINTRAC and other competent authorities, where required;
- conducting detailed analysis of transactions and customer activity as part of internal investigations;
- maintaining appropriate documentation and audit trails of investigations performed;
- performing other functions as assigned under internal policies, procedures, and job responsibilities.

The Investigation Unit ensures that all cases are reviewed in a timely, consistent, and risk-based manner, and that findings are properly documented and escalated where necessary.

Audit Function

The Company will establish an audit function to perform periodic and independent reviews of its AML/CTF framework in order to assess its effectiveness, adequacy, and compliance with applicable legal and regulatory requirements.

The frequency, scope, and depth of such reviews are determined based on the Company's risk profile, size, complexity, and regulatory expectations.

Where appropriate, the Company may engage independent external auditors to conduct or support such reviews.

The audit function is based on the following principles:

- independence of the audit and compliance functions in both structure and practice;
- regular review of the AML/CTF framework, conducted at least annually or more frequently where required by risk considerations;
- involvement of qualified internal or external parties with sufficient expertise;
- direct and unrestricted reporting lines to Senior Management and, where applicable, governing bodies or committees.

The audit results, including identified deficiencies and recommendations, shall be formally documented and communicated to Senior Management.

Senior Management is responsible for ensuring that appropriate remedial actions are taken within reasonable timeframes and that follow-up reviews are conducted where necessary.

While audit frequency may be adjusted based on risk considerations, the Company ensures that a comprehensive review of the AML/CTF framework is conducted at least once every two years in accordance with regulatory requirements.

Risk-Based Approach (RBA)

The Company applies a risk-based approach (RBA) to ensure that measures to prevent and mitigate money laundering and terrorist financing risks are proportionate to the nature and level of risks identified.

This approach enables the Company to allocate resources efficiently and to prioritize higher-risk areas, ensuring that enhanced controls are applied where they are most needed.

The Company assesses inherent risks by taking into account factors including, but not limited to:

- the nature of products, services, and technologies used;
- the type and profile of customers;
- geographic exposure and jurisdictions involved;
- transaction volumes, frequency, and patterns;
- the nature and purpose of business relationships.

Risks are not static and may evolve over time; therefore, the Company ensures continuous reassessment of risk profiles based on updated information and observed activity.

Risk assessment is conducted both:

- at the onboarding stage, to understand the customer's profile, business activities, and geographic connections;
- on an ongoing basis, to ensure that the assigned risk level remains appropriate throughout the business relationship.

The Company determines the extent and intensity of Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), and ongoing monitoring measures based on the assessed level of risk.

This ensures that preventive and mitigating controls are proportionate, effective, and aligned with regulatory expectations and industry best practices.

The application of the RBA enables the Company to apply proportionate controls by determining:

- the scope and depth of due diligence measures applied to each customer;
- the level of verification required for beneficial owners and persons acting on behalf of the customer;
- the intensity and frequency of ongoing monitoring of customer activity;
- the nature and extent of additional risk mitigation measures applied to higher-risk relationships.

The Company ensures that higher-risk customers, transactions, and jurisdictions are subject to enhanced scrutiny and additional controls, while lower-risk relationships are managed using simplified and proportionate measures, where permitted by applicable laws.

Risk-Based Approach at Customer Level

The application of a risk-based approach (RBA) involves identifying, assessing, and categorizing money laundering and terrorist financing (ML/TF) risks at the customer level, and implementing proportionate measures based on the risks identified.

The RBA does not prohibit the Company from entering into business relationships or conducting transactions; rather, it enables the Company to effectively manage and mitigate ML/TF risks through appropriate controls.

Risk Assessment and Risk Categories

The Company establishes, documents, and regularly updates its risk assessment framework in order to identify, assess, analyze, and manage ML/TF risks associated with its customers, products, services, and geographic exposure.

The risk assessment process is an integral part of the Company’s overall risk management framework and is applied consistently across all stages of the customer lifecycle.

The risk assessment process includes, at a minimum, the following stages:

- identification of relevant risk factors;
- analysis of identified risk factors;
- evaluation and classification of risks.

The Company applies both qualitative and, where appropriate, quantitative criteria to assess the level of risk.

Risk assessment is conducted:

- prior to establishing a business relationship (onboarding stage);
- on an ongoing basis throughout the duration of the relationship;
- upon the occurrence of triggering events (e.g., changes in customer profile, unusual activity, or regulatory updates).

The Company assigns each customer a risk rating (e.g., low, medium, high) based on the outcome of the risk assessment.

Risk categorization takes into account, among other factors:

- customer type and legal structure;
- beneficial ownership and control structure;
- geographic location and jurisdictional risk;
- nature of business activities;
- expected transaction behavior and volumes;
- use of intermediaries or third parties;
- delivery channels and technologies used.

The assigned risk level determines the extent of due diligence measures, the level of monitoring, and the frequency of review applied to each customer.

Sources of Risk Assessment

In the course of conducting risk assessments, the Company relies on multiple internal and external sources to ensure a comprehensive and informed evaluation of ML/TF risks. These sources include, but are not limited to:

- applicable laws and regulatory requirements, including Canadian legislation and FINTRAC guidance;
- national and international risk assessments, including publicly available reports;
- guidance issued by competent authorities and international organizations (including FATF);
- internal knowledge, expertise, and experience obtained through the Company's operations and similar business activities.

The Company ensures that risk assessments are based on up-to-date, reliable, and relevant information.

Customer Risk

The Company assesses the ML/TF risk of each customer by assigning an individual risk rating, taking into account a range of customer-specific risk factors.

Customer risk relates to the characteristics of the customer and, where applicable, its beneficial owners, including their identity, behavior, background, and business profile.

When assessing customer risk, the Company considers, among other factors:

- the customer's legal status, including whether the customer is a regulated entity, publicly listed company, governmental body, or financial institution;

- whether the customer or any related party qualifies as a Politically Exposed Person (PEP), or has known associations with PEPs (including family members or close associates);
- the complexity and transparency of the customer's ownership and control structure, including the use of holding structures, trusts, nominee arrangements, or bearer shares;
- any negative information or adverse media related to the customer or associated persons (e.g., regulatory findings, criminal records, sanctions exposure, or reputational concerns);
- the customer's behavior and overall profile, including consistency of provided information and general credibility;
- the nature of the customer's business activities, including whether such activities are cash-intensive or otherwise considered higher risk from an AML/CTF perspective;
- the origin of the customer's funds and wealth, and the ability to reasonably verify their legitimacy.

The Company applies enhanced scrutiny to customers presenting higher risk characteristics and ensures that such risks are appropriately mitigated through additional due diligence and monitoring measures.

Country or Geographic Risk

Country or geographic risk relates to risks arising from the jurisdiction associated with the customer, its beneficial owners, business activities, or transaction counterparties.

Such risks may stem from differences in regulatory frameworks, enforcement practices, levels of corruption, or exposure to financial crime and terrorist financing.

When assessing geographic risk, the Company considers, among other factors:

- the customer's country of residence, incorporation, and principal place of business;
- the location of counterparties involved in transactions;
- whether the jurisdiction is identified by the Financial Action Task Force (FATF) as having strategic AML/CTF deficiencies (including high-risk and monitored jurisdictions);

- whether the jurisdiction is subject to sanctions, embargoes, or restrictive measures imposed by Canada, the United Nations, or other relevant authorities;
- the level of corruption, criminal activity, or regulatory weakness associated with the jurisdiction;
- whether the jurisdiction is known to have links to terrorist financing or organized crime;
- whether the jurisdiction is considered high-risk based on internal risk assessments or credible external sources.

The Company applies enhanced due diligence and, where necessary, restrictions or prohibitions when dealing with customers or transactions connected to high-risk jurisdictions.

Product and/or Services Risk

Product and/or services risk relates to the nature of the products or services offered by the Company and how they may be used, misused, or exploited for ML/TF purposes.

Certain products or services may inherently present higher risks due to their characteristics, including speed, complexity, anonymity, or cross-border functionality.

When assessing product and service risk, the Company considers:

- the volume, frequency, and value of transactions associated with the product or service;
- transaction patterns, including indicators aligned with known typologies or red flags (e.g., FATF guidance);
- the intended purpose and expected use of the product or service;
- the potential for the product or service to be used in activities vulnerable to money laundering or terrorist financing;
- whether the product or service enables or increases anonymity or reduces transparency;
- the use of innovative technologies, new delivery channels, or emerging financial instruments that may increase ML/TF risk;
- the level of control and monitoring the Company is able to apply to the product or service.

The Company ensures that higher-risk products and services are subject to proportionate controls, including enhanced monitoring, transaction limits, and additional due diligence measures.

Delivery / Distribution Channel Risk

Delivery or distribution channel risk relates to the methods and channels used by the Company to deliver its products and services, onboard customers, and execute transactions.

These risks arise from the level of direct interaction with the customer, the degree of reliance on third parties, and the potential for anonymity, impersonation, or misuse of technology.

The Company recognises that non-face-to-face business relationships and digital channels may present increased ML/TF risks and therefore require enhanced controls and monitoring.

When assessing delivery channel risk, the Company considers the following factors:

- the method used to verify the identity of the customer and, where applicable, its representatives (e.g. face-to-face verification, remote onboarding, reliance on third-party verification providers);
- the involvement of regulated financial institutions, payment service providers, or intermediaries in the transaction chain;
- the reliability and integrity of the identification and authentication methods applied (including electronic KYC and digital identity solutions);
- the use of IP addresses, device identifiers, geolocation data, and other technical indicators associated with the customer;
- the use of technologies or tools that may obscure identity or location (e.g. VPNs, TOR networks, anonymisation tools, disposable or one-time wallets, encrypted communication channels);
- the level of automation in onboarding and transaction execution processes;
- the use of new or emerging technologies, digital platforms, or alternative distribution channels;
- the extent to which the Company can monitor, control, and verify activities conducted through the channel.

The Company applies a risk-based approach to delivery channels and ensures that higher-risk channels are subject to enhanced due diligence, stricter verification procedures, and increased transaction monitoring.

Where the risks associated with a particular delivery channel cannot be adequately mitigated, the Company reserves the right to restrict or decline the use of such channels.

Determination of the Customer's Risk Profile

The Company establishes and maintains a comprehensive list of risk factors as a separate document (Annex 3), which serves as the basis for determining the customer's risk profile.

The customer's risk profile is assessed at the onboarding stage and is continuously reviewed and updated throughout the business relationship, taking into account changes in the customer's behaviour, transaction patterns, and other relevant circumstances.

The risk assessment is conducted using a risk-based approach (RBA) and is based on a combination of factors, including, but not limited to:

- customer-related risk factors;
- geographic risk factors;
- product and service risk factors;
- delivery channel risk factors.

The Company applies a structured methodology to assign an appropriate risk rating to each customer (e.g. low, medium, high), ensuring that the level of due diligence and ongoing monitoring is proportionate to the identified level of risk.

Higher-risk customers are subject to enhanced due diligence (EDD), increased scrutiny, and more frequent monitoring, while lower-risk customers may be subject to simplified measures where permitted by applicable laws and regulations.

The risk profiling process is supported by internal systems, controls, and documented procedures to ensure consistency, transparency, and auditability of decisions.

The Company ensures that risk assessments are properly documented and that any changes to a customer's risk profile are justified, recorded, and approved in accordance with internal policies.

Maintaining the Customer's Risk Profile

The Company continuously monitors and reviews the business relationship with each customer to ensure that the assigned risk profile remains accurate, relevant, and up to date.

Customer risk profiles are reviewed on a periodic basis, as well as on a trigger-event basis, to reflect any material changes in the customer's circumstances, behaviour, or risk exposure.

Such reviews take into account, among other factors:

- changes in the customer's identity, ownership structure, or beneficial ownership;
- changes in the nature, scale, or purpose of the customer's business activities;
- deviations from expected transaction patterns or unusual account activity;
- new information obtained through ongoing monitoring, screening, or external sources (e.g. adverse media);
- changes in geographic exposure or involvement of higher-risk jurisdictions;
- updates in applicable laws, regulations, or internal risk assessment criteria.

The Company applies a structured review schedule based on the customer's risk level:

- High-risk customers - subject to enhanced and more frequent reviews;
- Medium-risk customers - subject to periodic reviews;
- Low-risk customers - subject to standard review cycles, unless trigger events occur.

Where a change in risk profile is identified, the Company updates the customer's risk rating accordingly and applies appropriate measures, including enhanced due diligence (EDD), additional verification, or restrictions where necessary.

All reviews, decisions, and changes to customer risk profiles are properly documented and retained in accordance with record-keeping requirements.

Non-Acceptable Customers

The Company has established and maintains a list of prohibited risk factors, the presence of which indicates that a customer falls outside the Company's risk appetite.

Where such risk factors are identified during customer onboarding or prior to the execution of an occasional transaction, the Company will refuse to establish a business relationship or to carry out the transaction.

If a prohibited risk factor is identified during an existing business relationship, the Company will take appropriate measures, including, where necessary, the termination of the relationship, in accordance with applicable laws, regulatory requirements, and internal procedures.

Prohibition of Anonymous Accounts

The Company strictly prohibits the opening or maintaining of anonymous accounts or accounts under fictitious, false, or misleading names.

The Company does not establish or continue a business relationship without obtaining sufficient and reliable information to verify the identity of the customer and, where applicable, the beneficial owner.

Where there are reasonable grounds to suspect that identification data, documentation, or information provided by the customer is false, altered, or misleading, the Company will:

- refuse to onboard the customer or execute the transaction;
- consider filing a report to the competent authority, where required;

- apply enhanced scrutiny and internal escalation procedures.

Prohibition of Shell Banks

The Company does not establish or maintain correspondent or business relationships with shell banks.

A shell bank is defined as a financial institution that has no physical presence in any jurisdiction and is not affiliated with a regulated financial group that is subject to effective consolidated supervision.

The Company takes reasonable measures to ensure that it does not enter into or maintain relationships with institutions that:

- lack a meaningful physical presence (mind and management) in any jurisdiction;
- do not have adequate governance, organizational structure, or internal control systems;
- are not subject to effective supervision by competent regulatory authorities.

The Company also ensures that it does not engage with financial institutions that permit their accounts to be used by shell banks.

Customer Due Diligence (CDD)

Customer Due Diligence (CDD) is a fundamental component of the Company's AML/CTF framework and is essential for effective identification, assessment, and mitigation of money laundering and terrorist financing risks.

The Company applies CDD measures to identify and verify each customer, as well as, where applicable, the beneficial owner, prior to establishing a business relationship or executing a transaction.

The purpose of CDD is to enable the Company to:

- assess the ML/TF risk associated with each customer;

- determine whether to establish or continue a business relationship or execute a transaction;
- define the appropriate level of due diligence (standard, simplified, or enhanced);
- determine the nature and extent of ongoing monitoring required.

CDD measures include, but are not limited to:

- identification and verification of the customer's identity using reliable and independent sources;
- identification and verification of the beneficial owner and understanding of the ownership and control structure (for legal entities);
- obtaining information on the purpose and intended nature of the business relationship;
- screening against sanctions lists, PEP databases, and adverse media;
- assessing the customer's risk profile in accordance with the Company's risk-based approach.

The Company ensures that CDD is conducted:

- prior to onboarding;
- on an ongoing basis throughout the business relationship;
- when there are changes in customer information or behavior;
- when a transaction appears unusual or suspicious.

Where the Company is unable to complete CDD measures to a satisfactory standard, it will:

- refuse to establish the business relationship or execute the transaction;
- terminate the existing relationship, where appropriate;
- consider submitting a report to the competent authority in accordance with applicable regulations.

Customer Due Diligence Measures

The Company applies the following Customer Due Diligence (CDD) measures in accordance with applicable AML/CTF legislation and regulatory guidance:

- identification of the customer and verification of the customer's identity using reliable, independent, and prescribed sources and methods to ensure the accuracy of the information provided;
- identification of the beneficial owner and taking reasonable measures to verify their identity, ensuring that the Company understands and is satisfied with the ownership and control structure of the customer, including in the case of legal entities, trusts, or similar arrangements;
- identification and assessment of whether the customer or beneficial owner is a Politically Exposed Person (PEP), Head of International Organization (HIO), or a person associated with such individuals (e.g., family members or close associates);
- obtaining information on the purpose and intended nature of the business relationship or transaction, unless such purpose and nature are already evident;
- conducting ongoing monitoring of the business relationship, including scrutiny of transactions to ensure consistency with the customer's profile and risk level.

Acting on Behalf of a Customer

Where a person purports to act on behalf of a customer, the Company shall:

- identify such person and take reasonable measures to verify their identity using reliable and independent documentation, data, or information;
- verify that the person is duly authorized to act on behalf of the customer, including obtaining appropriate supporting documentation (e.g., power of attorney, corporate authorization).

Situations Requiring CDD Measures

CDD measures shall be applied in the following circumstances:

- upon establishment of a business relationship;
- when conducting a transaction involving cash or virtual currency in an amount equal to or exceeding USD 10,000 within a 24-hour period (whether as a single transaction or a series of related transactions);

- where there are reasonable grounds to suspect that a transaction or attempted transaction is related to money laundering or terrorist financing, regardless of any thresholds or exemptions, and prior to submitting a Suspicious Transaction Report (STR);
- when issuing or redeeming negotiable instruments (such as traveller's cheques, money orders, or similar instruments) in the amount of USD 3,000 or more;
- where there are doubts about the veracity or adequacy of previously obtained customer identification data;
- when there is a material change in the customer's circumstances or risk profile.

Additional Triggers for Applying CDD Measures

In addition to the general cases outlined above, the Company applies CDD measures in the following situations:

- upon transmitting funds in the amount of USD 1,000 or more through an informal value transfer system (IVTS), including systems that transfer value without the physical movement of funds (e.g., hawala-type arrangements);
- upon initiating an electronic funds transfer (EFT) of USD 1,000 or more;
- upon conducting foreign currency exchange transactions exceeding USD 3,000 or virtual currency exchange transactions exceeding USD 1,000;
- upon executing or facilitating virtual currency transactions where the total value exceeds USD 10,000;
- upon remitting funds of USD 1,000 or more to a beneficiary via international funds transfer or IVTS;
- upon the creation of an initial information record in the course of providing crowdfunding platform services;
- upon processing or maintaining crowdfunding platform donations exceeding USD 1,000.

Timing of Customer Due Diligence

The Company ensures that all required CDD measures are completed prior to:

- establishing a business relationship;
- carrying out any occasional transaction subject to CDD requirements.

At a minimum, the following information must be obtained and verified before onboarding or transaction execution:

- customer identification data;
- beneficial ownership information (where applicable);
- PEP/HIO status and associated risk indicators;
- purpose and intended nature of the business relationship or transaction.

Where the Company is unable to complete CDD measures in full, it shall:

- refrain from establishing the business relationship;
- decline or suspend the transaction;
- terminate any existing relationship, where applicable;
- consider submitting a Suspicious Transaction Report (STR) to FINTRAC or other competent authority, where there are reasonable grounds for suspicion.

Establishment of Business Relationship

A business relationship is considered to be established when:

- the Company enters into a contractual arrangement with the customer for the provision of services; or
- repeated or ongoing transactions indicate a continuing relationship rather than a one-off interaction.

Where applicable, the Company may rely on previously obtained identification data, provided that:

- such data remains accurate, complete, and up to date;
- a re-verification is conducted within an appropriate timeframe (e.g., within five years or earlier based on risk level).

Services Subject to CDD Requirements

Customer Due Diligence (CDD) measures apply to the following services provided by the Company:

- virtual currency services;
- issuance of negotiable instruments (e.g., money orders, traveller's cheques);
- foreign exchange transactions;
- transmission of funds by any means, including domestic and international transfers

Keeping Customer Information Up to Date

The Company ensures that customer information obtained during onboarding remains accurate, complete, and up to date throughout the duration of the business relationship.

To achieve this, the Company conducts periodic reviews of customer records, applying a risk-based approach to determine the frequency and scope of such reviews.

CDD information must be reviewed and updated in particular when one or more of the following trigger events occur:

- a defined review period has elapsed, based on the customer's risk classification;
- the customer notifies the Company of changes to identification or profile information (e.g., name, address, occupation, business activity, ownership structure);
- a significant transaction occurs, including transactions that are large, unusual, or inconsistent with the customer's profile;
- there is a material change in the way the customer's account or relationship is used;
- the Company identifies deficiencies or inconsistencies in the customer's existing documentation or data;
- the Company becomes aware that it lacks sufficient or reliable information about the customer;
- there is a change in applicable legal or regulatory requirements affecting customer identification or verification standards.

Ongoing Screening and Monitoring

In addition to periodic reviews, the Company performs continuous screening of customers against relevant watchlists, including:

- sanctions lists;

- politically exposed persons (PEP) databases;
- adverse media sources.

Screening is conducted on an ongoing basis, including when relevant watchlists are updated or when new information becomes available.

Where a match or potential match is identified, the Company:

- performs enhanced due diligence (EDD) as appropriate;
- reassesses the customer's risk profile;
- determines whether further action is required, including reporting to the competent authority.

Exceptions to the Application of CDD Requirements

Where the Company has previously identified and verified a customer in accordance with applicable CDD requirements and maintains complete and reliable records, it may rely on such previously obtained information without repeating full CDD measures, provided that:

- there are no doubts regarding the accuracy, completeness, or validity of the existing information;
- the customer's risk profile remains unchanged;
- the information is reviewed and updated where necessary in accordance with the Company's risk-based approach.

In such cases, the Company may perform a simplified review and update of customer information (e.g., name, address, business activity), rather than full re-identification.

Specific Cases Where CDD May Not Be Re-applied

Subject to applicable laws and provided that no ML/TF suspicion arises, the Company may refrain from re-applying full CDD measures in the following limited circumstances:

- where the customer is a regulated financial institution or public body and transactions (including those exceeding USD 10,000) are conducted through regulated channels or accounts;
- where virtual currency transactions exceeding applicable thresholds are conducted by or with regulated financial institutions or public bodies;
- where the Company transfers or receives virtual currency solely as a technical component of transaction validation (e.g., blockchain validation rewards) with no underlying customer relationship risk;
- where the Company processes nominal or technical virtual currency transfers required only for transaction validation or data transmission purposes;
- where the Company has already verified the customer's identity and there are no doubts as to its accuracy, and repeating CDD would create a risk of "tipping-off" in the context of a suspicious transaction;
- where transactions occur within a formal employment relationship (e.g., employer–employee payments under a service or employment agreement), provided such activity does not present elevated ML/TF risk;
- where the customer is a large, well-established entity (e.g., public body, corporation, or trust with significant net assets), and sufficient reliable information is publicly available or has already been verified.

Limitations of CDD Exceptions

The above exceptions shall not apply in the following cases:

- where there are reasonable grounds to suspect money laundering or terrorist financing;
- where the Company has doubts about the accuracy or adequacy of previously obtained information;
- where there is a material change in the customer's risk profile;
- where required by applicable legislation or regulatory instructions.

In all such cases, the Company shall immediately apply full CDD or Enhanced Due Diligence (EDD) measures as appropriate.

Know Your Customer (KYC): Onboarding Principles

The Company has established a comprehensive customer onboarding procedure, documented separately, which defines the steps required for the application of Customer Due Diligence (CDD) measures.

This procedure outlines the requirements for collection, verification, and validation of customer information and documentation prior to establishing a business relationship.

The onboarding process is designed to ensure full compliance with applicable AML/CTF laws and reflects the Company's risk-based approach.

Identification of the Customer – Natural Person

During the onboarding process, the Company identifies and verifies the identity of each customer who is a natural person, and, where applicable, any person acting on their behalf.

Verification is conducted using reliable, independent source documents, data, or information appropriate to the selected verification method.

Methods of Identity Verification

The Company may apply one or more of the following methods for verifying the identity of a natural person:

- Government-issued photo identification method (including remote verification where permitted);
- Credit file method (using trusted credit bureau data);
- Dual-process method (verification through a combination of independent data sources);
- Affiliate or member method (where applicable within regulated frameworks);
- Reliance method (relying on identification performed by a third party, subject to regulatory requirements).

The choice of method is determined based on the customer's risk profile, geographic location, and the nature of the services provided.

Government-Issued Photo Identification Method

Where the Company relies on a government-issued photo identification method, it shall collect and retain sufficient information to reliably identify and verify the customer.

At a minimum, the following information must be obtained:

- full legal name of the individual;
- a clear image of the individual's photograph as shown on the identification document;
- document number, issuing authority, and expiry date (where applicable);
- confirmation that the document is valid and has not expired.

Where remote identification is used, the Company shall implement appropriate safeguards to ensure authenticity, including biometric checks, liveness detection, or equivalent technologies where applicable.

Additional Identification Data and Document Requirements

As part of the government-issued photo identification method, the Company records and retains the following additional information:

- date of verification;
- type of identification document;
- unique identification number of the document;
- issuing authority, place of issue, and expiry date (where applicable).

Acceptable Identification Documents

The following documents may be used as a valid basis for the identification and verification of a natural person, provided they contain the required data elements:

- government-issued identity card or citizenship document issued by Canada;
- identity document issued by a foreign government, provided it is equivalent in reliability and integrity to a Canadian-issued document;
- Canadian permanent resident card;
- Canadian provincial or territorial driver's licence.

Document Validation Requirements

All identification documents must meet the following criteria in order to be accepted:

- be authentic, valid, and not expired;
- be issued by a federal, provincial, territorial, or recognized foreign government authority;
- clearly indicate the individual's full legal name;
- include a clear photograph of the individual;
- contain a unique identifying number;
- correspond to the individual presenting the document (i.e., name and physical appearance must match).

The Company must take reasonable steps to verify the authenticity of the document, including assessing visible security features and ensuring that the document has not been altered, forged, or otherwise tampered with.

Unacceptable Documents

Documents are considered unacceptable where:

- they are issued by municipal or local authorities lacking sufficient reliability;
- they are expired, incomplete, or appear altered or falsified;
- they do not contain the minimum required identification elements (e.g., photo, unique number).

Verification Process

Where verification is conducted in person, the Company must examine the original physical document and assess its security features.

Where remote verification is applied, the Company must implement additional safeguards, such as:

- biometric verification (e.g., facial recognition and liveness checks);
- validation against trusted databases or registries;
- fraud detection tools to identify manipulated or synthetic documents.

The Company must ensure that the level of verification applied is proportionate to the assessed risk of the customer and consistent with applicable AML/CTF regulatory requirements.

Remote Government-Issued Photo Identification Method

Where a customer, and where applicable their representative, is identified without physical presence (remote onboarding), the Company applies a remote identification procedure based on government-issued photo identification, supplemented by additional authentication measures.

This procedure enables the Company to verify the authenticity and validity of the identification document using reliable technological solutions and independent verification methods.

Document Verification Process

As part of remote identification, the Company performs the following steps:

- requests a clear scan or photo of the customer's identification document;
- uses technological solutions to verify the document's authenticity by analysing:
    - visual characteristics (e.g., size, layout, font, spacing);
    - embedded security features (e.g., holograms, watermarks, chips);
    - official markers (e.g., logos, symbols);
- validates that the document is genuine, unaltered, and consistent with known document standards.

Customer Identity Verification (Liveness & Matching)

To ensure that the document belongs to the customer and is currently valid, the Company applies one of the following verification methods:

- live video verification
  The customer participates in a real-time video session where:
    - their facial image is captured;
    - the original identification document is presented and examined;
    - the session may be recorded for audit and compliance purposes;
- biometric (selfie-based) verification
  The customer:
    - submits a live photo ("selfie") using a secure application;
    - undergoes facial recognition and liveness detection checks;
    - is matched against the photograph contained in the identification document.

Use of Technological Solutions

Remote onboarding technologies may be used only where:

- the Company has formally approved a list of acceptable technological solutions, endorsed by Senior Management and the Compliance Officer;

- such technologies meet reliability, security, and regulatory standards;
- the onboarding procedure clearly defines how and when such technologies are applied;
- appropriate safeguards are in place to prevent identity fraud, spoofing, and document manipulation.

Compliance and Control Requirements

The Company ensures that:

- remote identification measures are proportionate to the customer's risk profile;
- higher-risk customers are subject to enhanced verification measures;
- all identification data, recordings, and verification results are securely stored and retained in accordance with applicable AML/CTF regulations;
- audit trails are maintained to demonstrate compliance with regulatory requirements.

Application of Measures

The Company shall apply at least one of the above verification methods.
Where risk factors are elevated or inconsistencies are detected, the Company reserves the right to require additional verification or revert to in-person identification.

Credit File Method

Where the Company applies the credit file method for customer identification and verification, it shall obtain and retain sufficient information to reliably confirm the customer's identity using independent and credible sources.

Data Collection Requirements

The Company shall collect and retain, at a minimum, the following information:

- full legal name of the individual;
- residential address;
- date of birth;
- credit file reference number (if applicable);
- date on which the credit file was accessed;
- name of the credit bureau or authorized third-party provider.

Source of Information

The Company shall:

- obtain credit file information directly from a recognized and reliable credit bureau or an authorized third-party provider;
- independently collect identifying information from the customer and compare it against the credit file data;
- ensure that the verification is performed at the time of onboarding or identity confirmation.

Credit file information may only be sourced from:

- Equifax Canada;
- TransUnion Canada;
- or other duly authorized and regulated third-party providers.

Verification Requirements

In order for a credit file to be considered valid for identification purposes, it must:

- contain accurate, current, and complete information;
- be obtained from a Canadian credit bureau (foreign credit bureaus are not acceptable);
- have been in existence for a minimum period (typically at least 3 years);
- include information derived from multiple independent and reliable sources;

- match the customer's name, address, and date of birth.

Control Measures and Validation

The Company shall ensure that:

- appropriate internal controls are in place to validate the reliability and integrity of the credit file data;
- discrepancies between customer-provided information and credit file data are identified and investigated prior to onboarding;
- the use of the credit file method is proportionate to the assessed risk level of the customer;
- additional verification measures are applied where:
    - the customer is classified as higher risk;
    - the credit file is insufficient, incomplete, or inconsistent.

Limitations of Use

The credit file method shall not be used:

- where sufficient credit history is not available;
- where the reliability or integrity of the data cannot be reasonably established;
- as a standalone method for higher-risk customers, unless supplemented by additional identification measures.

Additional Considerations for Credit File Matching

When comparing customer-provided information with data obtained from a credit file, the Company shall assess and document any discrepancies, including but not limited to:

- minor typographical errors in the name or address;
- discrepancies in the date of birth;
- presence of multiple addresses associated with the individual.

The Company applies a risk-based approach when evaluating such discrepancies:

- minor typographical errors (e.g., spelling variations) may be considered acceptable, provided there is no indication of fraud or identity inconsistency;
- discrepancies in the date of birth are considered material and shall prevent reliance on the credit file as a sole method of identification;
- the presence of multiple addresses may be acceptable where the credit file indicates a primary and secondary address or reflects a reasonable history of residence.

Where discrepancies cannot be reasonably explained or resolved, the Company shall apply additional verification measures or use an alternative identification method.

Dual-Process Method

The dual-process method involves the use of two independent categories of information obtained from two separate and reliable sources to verify a customer's identity within a single onboarding process.

Verification Approach

Under the dual-process method, the Company shall obtain and verify at least two of the following combinations of information:

- customer's name and residential address;
- customer's name and date of birth;
- customer's name and confirmation of a financial account (e.g., deposit account, prepaid product, credit card, or loan account with a financial institution).

These data elements must be verified against reliable and independent sources.

Combination of Data

The Company shall combine two different categories of information, for example:

- name and address + name and date of birth;
- name and address + financial account confirmation;
- name and date of birth + financial account confirmation.

The Company must ensure that all information:

- matches the data provided by the customer;
- is consistent across sources;
- does not contain unexplained discrepancies.

Source Requirements

For the dual-process method:

- each category of information must be obtained from a different independent source;
- the same source must not be used for both data points;
- all sources must be reliable, current, and verifiable;
- acceptable sources shall be defined in a separate internal document (e.g., Annex).

Control and Validation Measures

The Company shall ensure that:

- the information used is valid, up-to-date, and derived from credible sources;
- any inconsistencies are investigated prior to onboarding;

- higher-risk customers are subject to enhanced verification measures;
- audit trails are maintained documenting:
    - sources used;
    - verification steps performed;
    - outcome of the identification process.

Limitations of Use

The dual-process method shall not be used:

- where independent sources cannot be obtained;
- where data is outdated, incomplete, or unreliable;
- as a standalone method for higher-risk customers without additional safeguards.

Affiliate or Member Method

Where the Company applies the affiliate or member method for customer identification and verification, it may rely on information obtained from an affiliated entity or member organization, provided that such reliance meets applicable AML/CTF requirements.

Data Collection Requirements

The Company shall obtain and retain, at a minimum, the following information:

- full legal name of the individual;
- residential address;
- date of birth;
- records and confirmation obtained from the affiliate or member entity.

Eligible Entities

The Company may rely on information provided by the following entities:

- an affiliate of the Company that conducts activities regulated under applicable AML/CTF legislation (e.g., PCMLTFA);
- a foreign affiliate, provided it is subject to equivalent AML/CTF regulatory requirements and oversight;
- a financial institution that is a member of the same financial services group, cooperative, or credit union central.

Conditions for Reliance

The Company may rely on the affiliate or member method only where:

- the affiliate or member has previously verified the customer's identity using methods compliant with applicable AML/CTF requirements;
- the verification performed is equivalent to the standards required by the Company;
- the Company has reasonable assurance of the reliability of the affiliate's controls and procedures;
- there is a formal arrangement or internal policy governing such reliance.

Verification and Matching Requirements

The Company shall:

- compare and match the information received from the affiliate or member with the information provided directly by the customer;
- ensure consistency across all data points (name, date of birth, address, etc.);
- identify and investigate any discrepancies prior to onboarding.

Where inconsistencies, doubts, or deficiencies are identified, the Company shall:

- perform independent verification; or
- apply alternative identification methods in accordance with this Program.

Control and Oversight

The Company shall ensure that:

- reliance on affiliates or members is subject to ongoing monitoring and periodic review;
- the affiliate or member operates under equivalent AML/CTF standards;
- all reliance arrangements are properly documented;
- audit trails are maintained evidencing:
    - the source of information;
    - verification steps performed;
    - justification for reliance.

Limitations of Use

The affiliate or member method shall not be used:

- where the affiliate's AML/CTF framework is not demonstrably equivalent;
- where the Company cannot obtain sufficient information to verify identity independently if required;
- as a standalone method for higher-risk customers without additional verification measures.

Identification of the Customer: Legal Entity

The Company shall identify and verify the identity of customers that are legal entities, as well as their authorized representatives, using reliable, independent source documents, data, or information.

The identification of a legal entity includes, at a minimum:

- confirmation of the entity's legal existence;
- verification of the entity's name, registration number, and registered address;
- identification of individuals authorized to act on behalf of the entity;
- identification and verification of beneficial owners and control structure, where applicable.

Where the Company applies the confirmation of existence method, it shall verify that a legal entity exists and is active using reliable, independent, and up-to-date sources.

Data Collection Requirements

The Company shall obtain and retain, at a minimum, the following information:

- legal name of the entity;
- registered or principal business address;
- registration/incorporation number (where applicable).

Acceptable Sources of Verification

The Company may rely on the following documents or data sources to confirm the existence of a legal entity:

- partnership agreements;
- articles of incorporation / articles of association;
- certificates of incorporation or registration;
- the most recent official records confirming existence and containing the entity's name and address;
- extracts from publicly accessible and reliable corporate registries or official databases.

Document and Source Requirements

All documents and records used must:

- be authentic, valid, and current;
- originate from a reliable and independent source;
- contain sufficient information to confirm the legal existence of the entity;
- be consistent with the information provided by the customer.

Where discrepancies are identified, the Company shall perform additional verification or request further documentation.

Control Measures

The Company shall ensure that:

- verification is performed prior to establishing a business relationship;
- the entity is not dissolved, struck off, or inactive;
- any inconsistencies in corporate data are investigated;
- audit trails are maintained documenting the verification process and sources used.

Reliance Method

The Company may rely on information obtained from another entity (including affiliated entities or third parties) for the purposes of identifying and verifying a customer, provided that such reliance complies with applicable AML/CTF requirements.

Eligible Third Parties

The Company may rely on:

- entities subject to AML/CTF obligations under applicable legislation (e.g., PCMLTFA);
- affiliated foreign entities performing similar regulated activities, provided they are subject to equivalent AML/CTF standards.

Conditions for Reliance

The Company may rely on a third party only where:

- the third party has previously conducted CDD in accordance with applicable AML/CTF requirements;
- the Company obtains sufficient information immediately to confirm the customer's identity;
- the Company can obtain copies of underlying identification data and documents without delay upon request;
- the third party is subject to equivalent regulation, supervision, and compliance standards;
- a formal agreement or arrangement governs the reliance relationship.

Responsibility and Accountability

Notwithstanding reliance on a third party, the Company remains fully responsible for compliance with AML/CTF obligations, including:

- adequacy of customer identification;
- ongoing monitoring;
- reporting obligations.

Control and Risk Management

The Company shall ensure that:

- reliance arrangements are subject to periodic review and risk assessment;
- higher-risk customers are not onboarded solely on the basis of reliance;
- additional due diligence is applied where necessary;
- reliance is not used where there are doubts about the third party's reliability or data integrity.

Limitations of Use

The reliance method shall not be used:

- where the Company cannot obtain underlying documentation upon request;
- where the third party is located in a high-risk jurisdiction without equivalent AML/CTF standards;
- as a standalone method for high-risk customers.

Reliance Method: Additional Requirements and Verification

The Company may apply the reliance method only where it has established that the relied-upon entity (Reporting Entity or affiliated foreign entity):

- maintains documented AML/CTF policies, including procedures for customer identification, record-keeping, risk assessment, and enhanced due diligence for high-risk customers;
- is subject to supervision by a competent regulatory authority under applicable legislation in its jurisdiction.

Conditions for Use of Reliance

The reliance method may be applied only if all of the following conditions are met:

- the Company has obtained sufficient information from the other Reporting Entity (RE) or affiliated foreign entity used to verify the customer's identity;
- the Company has assessed and is satisfied that the information is accurate, valid, and up to date, and that the customer's identity has been verified in accordance with applicable standards;
- the Company has entered into a written agreement or arrangement with the third party requiring them to:
    - provide all relevant customer identification data and documentation upon request;
    - maintain AML/CTF compliance standards equivalent to those applicable to the Company;
- the Company is able to obtain underlying identification documents without delay upon request.

Verification and Data Cross-Check

The Company shall independently verify the accuracy of customer data by:

- cross-checking information against publicly accessible registers or other reliable and independent data sources;
- ensuring consistency between data received from the third party and data obtained from independent verification sources.

Where access to official registries is available, the Company may rely on such sources instead of requesting documents directly from the customer, provided that the data is sufficient and reliable.

The Company shall independently verify the accuracy of customer data by:

- cross-checking information against publicly accessible registers or other reliable and independent data sources;
- ensuring consistency between data received from the third party and data obtained from independent verification sources.

Where access to official registries is available, the Company may rely on such sources instead of requesting documents directly from the customer, provided that the data is sufficient and reliable.

Use of Electronic and Remote Verification

The Company may use electronic identification tools and trust services where:

- such tools are reliable, secure, and compliant with applicable legal standards;
- at least two independent sources are used for verification;
- appropriate controls are in place to detect fraud or manipulation.

Control Measures

The Company shall ensure that:

- reliance is not used for high-risk customers without additional due diligence;
- discrepancies or inconsistencies trigger enhanced verification measures;
- reliance arrangements are periodically reviewed and reassessed;
- full audit trail of reliance and verification steps is maintained.

Identification of the Customer's Representative and Verification of Authority

The Company shall identify any individual acting on behalf of a customer (the "Representative") and verify both the identity of such individual and the scope of their authority.

1. Identification of the Representative

The Representative shall be identified in the same manner as a natural person customer, in accordance with the Company's CDD procedures.

2. Types of Representatives (Legal Entities)

Where the customer is a legal entity, the following persons may be recognized as Representatives:

- a natural person whose authority arises by law or corporate governance documents (e.g., director, management board member, manager, or equivalent position) (the "Authorized Representative");
- a natural person acting on the basis of a valid power of attorney or other authorization issued by an Authorized Representative (the "Contractual Representative").

3. Verification of Authority

The Company shall:

- verify the existence and validity of the Representative's authority;

- determine the scope and limitations of such authority;
- ensure that the intended transaction or business relationship falls within that scope;
- retain records of the authorization used for verification.

Where the authority is confirmed via:

- official corporate registers;
- articles of association;
- or other reliable public sources,

the Company may rely on such sources without requiring additional authorization documents, provided sufficient evidence is obtained and retained.

4. Legalization and Jurisdictional Requirements

Where authorization documents are issued outside Canada:

- such documents must comply with applicable legal requirements for recognition (e.g., notarization, apostille, or legalization, where required);
- the Company shall assess whether the document is legally valid and enforceable in the relevant jurisdiction.

5. Control Principle

The Company shall provide services only within the verified scope of the Representative's authority and shall refuse or suspend transactions that exceed such authority.

Identification of the Customer’s Beneficial Owner

1. Definition

A beneficial owner is any natural person who:

- ultimately owns or controls the customer (legal entity or arrangement); or
- on whose behalf a transaction or activity is conducted.

2. Identification and Verification

The Company shall:

- identify all beneficial owners of the customer;
- take reasonable measures to verify their identity;
- understand the ownership and control structure of the customer.

Detailed procedures are set out in a separate document (Annex 6 – Beneficial Ownership Guidelines).

3. Information Collected

At a minimum, the Company shall collect the following information for each beneficial owner:

- full name (including surname);
- residential address;
- date of birth;
- nationality;
- ownership percentage and/or control nature;
- source of funds and, where applicable, source of wealth.

4. Risk-Based Approach

The level of verification shall depend on the assessed risk level:

- low/medium risk – reasonable measures and standard verification;
- high risk – enhanced due diligence, including:
  - independent verification sources;
  - additional supporting documentation;
  - deeper analysis of ownership/control structure.

Verification of Beneficial Ownership Information

The Company shall obtain from the customer sufficient information regarding the beneficial owner(s), supported by reliable documentation and independent sources.

To ensure accuracy and completeness, the Company shall:

- request beneficial ownership information directly from the customer, including supporting documentation;
- provide the customer with the opportunity to formally declare their beneficial owner(s) during onboarding;
- conduct independent verification, including:
  - open-source intelligence (OSINT);
  - publicly available registers;
  - corporate and ownership databases.

Confirmation of Ownership and Control Structure

The Company shall take reasonable and proportionate measures to verify the ownership and control structure of the customer, including:

- identifying whether the customer is part of a group structure;
- analyzing ownership layers and control mechanisms;
- reviewing official documentation, such as:
    - shareholder registers;
    - articles of incorporation;
    - constitutional documents;
    - board resolutions or equivalent records.

Where appropriate, the Company shall also assess management control in addition to ownership.

Fallback Measures (Where Beneficial Owner Cannot Be Identified)

If the Company is unable to identify or verify the beneficial owner(s):

- it shall identify and verify the identity of the senior managing official (e.g., CEO or equivalent);
- it shall apply Enhanced Due Diligence (EDD) measures;
- it shall document all steps taken to identify the beneficial owner;
- it shall assess whether the relationship presents an unacceptable risk.

Identification of the Purpose and Nature of the Business Relationship or Transaction

The Company shall obtain sufficient information to understand the purpose and intended nature of the business relationship or transaction.

This includes:

- understanding why the customer seeks to establish the relationship;
- identifying the expected use of products and services;
- assessing expected transaction patterns and volumes.

Standard Measures

Depending on the risk level, the Company may:

- require the customer to confirm acceptance of the Company's terms and conditions;
- request additional information regarding the nature of transactions and business activity;
- collect supporting documentation where necessary.

Enhanced Measures (Risk-Based Approach)

The Company shall apply additional measures where:

- transactions are of high value;
- transactions are unusual or inconsistent with the customer profile;
- the structure or activity appears complex or lacks transparency.

Such measures may include:

- obtaining additional documentation or explanations;
- performing deeper analysis of transaction purpose;
- applying ongoing enhanced monitoring.

Politically Exposed Persons (PEP) and Head of International Organization (HIO) Identification

1. Definition of PEP

A Politically Exposed Person (PEP) is a natural person who is or has been entrusted with prominent public functions.

This definition also includes:

- family members;
- close associates of such persons.

2. Prominent Public Functions

Prominent public functions include, but are not limited to:

- Head of State or Head of Government;
- Member of government, executive council, or legislature;
- Deputy minister or equivalent senior official;
- Ambassador, chargé d'affaires, or senior diplomatic official;
- Senior military officer (general rank or above);
- Senior executive of a state-owned enterprise or state-owned bank;
- Head of a government agency or regulatory authority;
- Judge of a supreme court, constitutional court, or equivalent high-level judicial body;
- Leader or senior official of a political party represented in a legislature.

3. Head of International Organization (HIO)

A Head of International Organization (HIO) is a natural person who holds or has held a senior leadership position within an international organization.

This definition also includes:

- family members;
- close associates of such persons.

4. Definition of International Organization

An international organization means:

- an organization established by the governments of multiple states;
- any institution or body operating under such an organization.

5. Identification and Screening Requirements

The Company shall:

- determine whether a customer or beneficial owner is a PEP, HIO, or related person;
- perform screening against:
    - PEP databases;
    - sanctions lists;
    - adverse media sources;
- document the results of such screening.

6. Risk Classification and Measures

Where a customer is identified as a PEP or HIO, the Company shall:

- classify the customer as high-risk;
- apply Enhanced Due Diligence (EDD) measures, including:
    - obtaining information on source of funds and source of wealth;
    - conducting enhanced background checks;
    - applying increased monitoring of transactions;
- obtain senior management approval prior to establishing or continuing the business relationship.

7. Ongoing Monitoring

The Company shall:

- conduct ongoing monitoring of PEP/HIO relationships;
- periodically review the status of the customer;
- reassess risk where:
    - the customer's role changes;
    - new information becomes available.

8. Former PEPs

Where a person is no longer entrusted with a prominent public function:

- the Company shall assess whether the risk associated with that person remains elevated;
- Enhanced Due Diligence measures may continue to apply based on a risk-based approach.

Close Family Members and Close Associates of PEP/HIO

1. Close Family Member

A Close Family Member of a PEP or HIO includes:

- spouse or common-law partner;
- children (biological or adopted);
- parents;
- siblings (brothers and sisters);
- spouses or partners of the above persons.

2. Close Associate

A Close Associate is a natural person who is closely connected to a PEP/HIO through personal, professional, or financial relationships.

This includes, but is not limited to, a person who:

- has a business relationship, joint ownership, or control over a legal entity together with a PEP/HIO;
- is known to have a close personal relationship with a PEP/HIO;
- is involved in financial transactions or arrangements with a PEP/HIO;
- holds a position within the same political organization, board, or structure as a PEP/HIO;
- is engaged in charitable or non-profit activities linked to a PEP/HIO;
- is listed as a joint holder, beneficiary, or signatory on financial products or arrangements connected to a PEP/HIO.

PEP/HIO Identification and Screening Process

The Company shall take reasonable measures to determine whether:

- the customer;
- the beneficial owner;
- or the customer's representative

is a PEP, HIO, Close Family Member, or Close Associate.

Methods Used

For this purpose, the Company shall:

- obtain a self-declaration from the customer during onboarding;
- verify information using:
  - publicly available sources;
  - official registers;
- perform screening against:
  - commercially available PEP databases;
  - sanctions lists;
  - adverse media sources.

All results must be documented and retained.

Ongoing Monitoring and Status Changes

The Company shall:

- monitor whether an existing customer becomes a PEP/HIO or related person;
- update the risk classification accordingly;
- apply Enhanced Due Diligence where required.

Former PEPs – Risk Retention Period

Where a customer is no longer a PEP:

- the Company shall continue to assess the risk associated with the individual for a minimum period of 5 years;
- during this period, a risk-based approach shall be applied;
- Enhanced Due Diligence may continue where residual risk remains.

The Company may only downgrade the risk classification once it has established that:

- the individual no longer holds influence;
- the risk factors associated with PEP status are no longer present.

Enhanced Due Diligence (EDD) Measures

The Company applies Enhanced Due Diligence (EDD) measures where the customer, transaction, or product/service presents a higher risk of money laundering or terrorist financing (ML/TF).

EDD is designed to:

- mitigate elevated ML/TF risks;
- obtain a deeper understanding of the customer and their activities;
- ensure ongoing monitoring is proportionate to the identified risk.

The scope and intensity of EDD measures shall be determined based on the nature, complexity, and severity of the identified risk.

High-Risk Situations Requiring EDD

The Company shall apply EDD measures in situations including, but not limited to:

- where the customer's risk profile is classified as high-risk;
- where there are doubts regarding:
  - the accuracy or completeness of customer information;
  - the authenticity of identification documents;
  - the identity of the beneficial owner;
  - the transparency of ownership/control structures (including complex or layered structures);
- where the customer is:
  - a financial institution involved in correspondent banking;
  - a financial institution that has been subject to sanctions or regulatory concerns;
- where the customer, beneficial owner, or representative is:
  - a PEP/HIO;
  - a family member or close associate of a PEP/HIO;
- where there are frequent or high-value transactions, especially involving:
  - cross-border transfers;
  - movement of funds through personal and business accounts;
- where transactions involve or are connected to:
  - high-risk jurisdictions;
  - financial secrecy jurisdictions;
- where the customer has links (residence, incorporation, counterparties, payment flows) to jurisdictions identified by credible sources (e.g., FATF, sanctions regimes, regulatory reports) as presenting elevated ML/TF risk.

EDD Measures Applied

In high-risk situations, the Company shall apply one or more of the following measures:

1. Enhanced Customer Identification

- obtaining additional identification documents;
- verifying identity using multiple independent sources;

2. Beneficial Ownership Deep-Dive

- obtaining detailed ownership structure;
- identifying ultimate beneficial owners through multiple layers;
- verifying ownership through independent sources;

3. Source of Funds and Source of Wealth

- obtaining information on:
  - origin of funds used in transactions;
  - overall wealth of the customer;
- supporting documentation may include:
  - bank statements;
  - contracts;
  - financial statements;

4. Purpose and Nature Verification

- obtaining detailed explanation of:
  - business activity;
  - expected transactions;
- verifying consistency with the customer profile;

5. Senior Management Approval

- obtaining approval from senior management prior to:
  - establishing the relationship;
  - continuing the relationship (if risk increases);

6. Enhanced Monitoring

- increased frequency of transaction monitoring;
- real-time or near real-time monitoring where appropriate;
- review of transaction patterns against expected behavior;

Ongoing Risk Management

The Company shall:

- continuously reassess high-risk relationships;
- update risk classification where new information arises;
- escalate suspicious activity in accordance with reporting obligations (e.g., STR/FINTRAC reporting).

Scope of Enhanced Due Diligence (EDD) Measures

Prior to applying Enhanced Due Diligence (EDD) measures, the Company ensures that a high-risk level has been appropriately identified and documented in relation to the customer, business relationship, or transaction.

Each identified risk factor may independently justify the application of EDD measures.

The scope, depth, and intensity of EDD measures shall be determined on a risk-based approach, taking into account:

- the nature of the customer;
- the complexity of the ownership and control structure;
- the type, size, and frequency of transactions;
- the geographic risk exposure;
- the product, service, or delivery channel involved.

EDD Measures Applied

Where EDD is required, the Company shall apply one or more of the following enhanced measures:

1. Enhanced Customer Information

- obtaining additional information about the customer, including:
  - occupation and professional background;
  - financial standing and estimated assets;
  - publicly available information (e.g., internet sources, corporate registries);

2. Purpose and Relationship Analysis

- obtaining detailed information on:
  - the purpose and intended nature of the business relationship;
  - expected account activity and transaction behavior;

3. Source of Funds (SoF) and Source of Wealth (SoW)

- collecting and verifying information regarding:
  - the origin of funds used in transactions;
  - the origin of the customer’s overall wealth;

4. Transaction Justification

- obtaining explanations and supporting documentation for:
  - specific transactions;
  - unusual or complex transaction patterns;

5. Additional Verification

- obtaining additional documents, data, or information;
- performing independent verification through reliable external sources;

6. Enhanced Monitoring

- applying increased frequency and depth of transaction monitoring;
- monitoring high-risk products, services, and channels more closely;

7. Risk Mitigation Controls

- establishing transaction limits or thresholds;
- applying restrictions on certain activities where necessary;
- strengthening internal controls over high-risk relationships;

8. Senior Management Involvement

- obtaining approval from senior management:
  - prior to establishing a high-risk relationship;
  - for ongoing or new high-risk transactions/products;

Governance and Documentation

The Company maintains a dedicated internal procedure for EDD measures (Annex [X]), which includes:

- criteria for triggering EDD;
- escalation procedures;
- documentation and record-keeping requirements;
- responsibilities of employees and compliance personnel.

All EDD actions must be properly documented, justified, and available for regulatory review.

High-Risk Third Countries

Where a customer, beneficial owner, or transaction is connected to a high-risk third country, as identified by the Financial Action Task Force (FATF) or other competent authorities, the Company shall apply Enhanced Due Diligence (EDD) measures proportionate to the level of risk identified.

High-risk third countries include jurisdictions with strategic deficiencies in AML/CTF frameworks, including those subject to increased monitoring or call for action by FATF.

Where a customer, beneficial owner, or transaction is connected to a high-risk third country, as identified by the Financial Action Task Force (FATF) or other competent authorities, the Company shall apply Enhanced Due Diligence (EDD) measures proportionate to the level of risk identified.

High-risk third countries include jurisdictions with strategic deficiencies in AML/CTF frameworks, including those subject to increased monitoring or call for action by FATF.

Additional Risk-Based Measures

Depending on the risk assessment, the Company may also:

- restrict certain products, services, or transaction types;
- apply transaction limits or thresholds;
- require additional documentation or independent verification;
- conduct adverse media and open-source intelligence checks;
- escalate the relationship for periodic senior review;

Ongoing Obligations

For customers linked to high-risk third countries, the Company shall:

- perform enhanced ongoing monitoring throughout the relationship;
- regularly reassess the customer's risk profile;
- update CDD information more frequently than for standard-risk customers;

Refusal or Termination

The Company shall not establish or shall terminate a business relationship where:

- sufficient information to mitigate ML/TF risk cannot be obtained;
- the source of funds or wealth cannot be reasonably verified;
- the risk remains unacceptably high after application of EDD measures.

Regulatory Alignment

This approach is aligned with:

- FATF Recommendations (in particular Recommendation 19);
- applicable Canadian AML/CTF requirements (FINTRAC);
- internal risk-based AML/CTF framework of the Company.

Source of Wealth and Source of Funds

Establishing the Source of Wealth (SoW) and Source of Funds (SoF) is a fundamental component of the Company's risk-based AML/CTF framework and a core requirement of Enhanced Due Diligence (EDD).

Establishing the Source of Wealth (SoW) and Source of Funds (SoF) is a fundamental component of the Company's risk-based AML/CTF framework and a core requirement of Enhanced Due Diligence (EDD).

Source of Funds refers to the origin of specific funds involved in a transaction or business relationship.

It aims to determine:

- where the funds used in a transaction originate from;
- whether such funds are legitimate and traceable;
- whether the transaction is consistent with the customer's profile and SoW.

Application of SoW and SoF

The Company applies SoW and SoF measures:

- at onboarding, particularly for medium- and high-risk customers;
- as part of Enhanced Due Diligence (EDD);
- in case of unusual, complex, or high-value transactions;
- where there are inconsistencies or red flags identified during monitoring;

Verification Measures

The Company shall obtain and verify SoW and SoF information using reliable, independent sources, which may include:

For Source of Wealth

- employment and income records;
- business ownership documentation;
- financial statements;
- investment portfolios;
- inheritance or gift documentation;
- publicly available information (e.g., registries, media);

For Source of Funds

- bank statements;
- transaction records;
- tax returns;
- contracts or agreements (e.g., sale of assets, dividends);
- payment confirmations;

Risk-Based Approach

The extent and depth of SoW and SoF verification shall be determined based on:

- the customer's risk classification;
- transaction size and frequency;
- jurisdictional risk;
- presence of PEP status or complex ownership structures;

For high-risk customers, the Company shall:

- obtain documentary evidence supporting SoW and SoF;
- independently verify the information obtained;
- apply enhanced scrutiny and ongoing monitoring;

Ongoing Monitoring

The Company shall ensure that SoW and SoF information remains:

- up-to-date;
- consistent with customer activity;

Where discrepancies arise, the Company shall:

- request additional information;
- reassess the customer's risk profile;
- apply further EDD measures where necessary;

Failure to Verify

Where the Company is unable to:

- adequately establish or verify SoW or SoF; or
- reasonably satisfy itself as to the legitimacy of funds;

the Company shall:

- not establish the business relationship; or
- terminate the existing relationship;
- consider filing a Suspicious Transaction Report (STR), where applicable.

Verification of Source of Funds and Supporting Documentation

The types of data and documentation used to verify the Source of Funds (SoF) and, where applicable, the Source of Wealth (SoW), may vary depending on the specific circumstances of the customer, the nature of the business relationship, and the level of risk identified.

The Company applies a risk-based approach and relies only on reliable, independent, and verifiable sources.

Acceptable Sources of Information

The following documents and data may be considered reliable for verification purposes, provided that their authenticity and relevance are reasonably established:

- government-issued or officially registered documents and data;

- bank statements and other financial institution records;
- payslips, salary statements, or employment income confirmations;
- tax returns and official tax assessments;
- inheritance documentation (e.g., probate documents, letters of administration);
- audited financial statements prepared by qualified accountants;
- documentation confirming business ownership or participation;
- written confirmation from regulated professionals (e.g., lawyers, accountants) with an established relationship with the customer;
- wills or estate-related documentation;
- contracts, including:
    - sale and purchase agreements;
    - service agreements;
    - loan agreements;
- invoices, proof of services rendered, or other commercial documentation;

Business Customers

For customers conducting business activities, the Company may additionally rely on:

- accounting records and balance sheets;
- contracts with counterparties;
- invoices and transaction documentation;
- proof of business operations and revenue generation;

Such documentation is used to establish a clear understanding of how funds have been generated and accumulated.

Threshold-Based Approach

The Company establishes transactional thresholds and triggers, upon exceeding which additional Source of Funds verification is required.

These thresholds are defined within the Company's transaction monitoring framework and may depend on:

- transaction size;
- frequency of transactions;
- customer risk profile;
- geographic risk factors;

Verification Standards

All documents and information used for verification must be:

- authentic, valid, and current;
- consistent with the customer's profile and declared activities;
- obtained from independent and credible sources, where possible;

Where necessary, the Company shall:

- request additional supporting documentation;
- perform independent verification;
- cross-check information across multiple sources;

Ongoing Monitoring

The Company continuously monitors customer activity and may request updated SoF/SoW information:

- where transaction behavior deviates from expected patterns;
- where new risk factors arise;
- at periodic review intervals depending on the risk classification;

Failure to Provide Adequate Evidence

Where the customer fails to provide sufficient or satisfactory evidence of Source of Funds or Source of Wealth, the Company shall:

- refrain from executing the transaction;
- decline to establish the business relationship; or
- terminate the existing relationship;

and, where appropriate:

- escalate the matter internally;
- consider filing a Suspicious Transaction Report (STR) in accordance with applicable laws and regulations.

Ongoing Monitoring

In the course of ongoing monitoring of the business relationship, the Company continuously monitors transactions carried out by customers to ensure that such transactions are consistent with the Company's knowledge of the customer, including the customer's business profile, risk level, source of funds, and transactional behavior as established during onboarding and updated throughout the relationship.

The Company applies a combination of automated transaction monitoring systems and manual review processes to detect unusual, complex, or suspicious activities. This includes identifying transactions that are inconsistent with the expected activity, lack apparent economic or lawful purpose, or deviate from the customer's known profile.

The Company also monitors customer activity to identify indicators of potential money laundering, terrorist financing, sanctions evasion, or other financial crime risks. Particular attention is given to:

- high-value transactions;
- unusual transaction patterns or volumes;
- rapid movement of funds (e.g., layering);
- transactions involving high-risk jurisdictions;
- use of multiple accounts or payment methods without clear rationale.

Where necessary, the Company reassesses the customer's risk profile on an ongoing basis. Any material changes in customer behavior, structure, ownership, or transaction patterns may result in a risk reclassification and the application of Enhanced Due Diligence (EDD) measures.

Transaction monitoring rules, thresholds, and escalation procedures are defined in a separate internal document (Transaction Monitoring Framework), which is regularly reviewed and updated to reflect regulatory expectations and risk developments.

Risk-Based Approach to Monitoring

The scope, intensity, and frequency of ongoing monitoring are determined based on the customer's risk profile.

The Company applies a risk-based approach, whereby higher-risk customers are subject to more frequent and enhanced monitoring measures. This includes, but is not limited to, politically exposed persons (PEPs), customers from high-risk jurisdictions, and customers with complex ownership structures.

As part of this approach, the Company considers the following factors:

- the nature, size, and frequency of transactions (including unusual spikes or deviations);
- the overall transaction patterns and behavioral trends over time;
- the value of transactions, with enhanced scrutiny applied to large or cumulative amounts;
- the geographical origin and destination of funds;

- the type of products and services used;
- the customer's declared business activity and expected turnover.

For high-risk customers, the Company performs enhanced monitoring, including more frequent reviews, deeper analysis of transactions, and verification of supporting documentation where required.

Screening and Monitoring Frequency

The Company conducts ongoing screening of its customer base against sanctions lists, PEP databases, and adverse media sources on a continuous basis through automated systems. In addition:

- real-time screening is applied during onboarding and transaction execution where applicable;
- periodic re-screening is conducted at least daily for sanctions and PEP updates;
- adverse media screening is refreshed periodically based on risk level (e.g., annually for standard risk, more frequently for high-risk customers).

Any matches or alerts are subject to immediate review by the Compliance function.

Additional Monitoring Considerations

In performing ongoing monitoring, the Company also takes into account:

- the customer's expected activity and declared turnover;
- known typologies and transaction patterns published by relevant authorities (including FATF, FINTRAC, and EU regulatory bodies);
- results derived from transaction monitoring tools and, where applicable, blockchain analytics or virtual asset screening solutions.

Monitoring of Changes in Customer Profile

The Company remains vigilant to changes in the customer's risk profile and business relationship over time. This includes identifying and assessing:

- entry into new products or services that may present higher ML/TF risk;
- changes in corporate structure, ownership, or control (including introduction of trusts or complex structures);
- material changes in the customer's declared activity, business model, or turnover;
- changes in transaction behavior, including increased volumes, frequency, or transaction size.

Where significant changes are identified, the Company performs a reassessment of the customer's risk profile and applies appropriate measures, including Enhanced Due Diligence (EDD), request for updated documentation, or escalation to the Compliance function.

Ongoing monitoring procedures are dynamically adjusted to reflect such changes and ensure that the Company maintains an up-to-date understanding of the customer and associated risks.

Methods and Procedures

In determining the appropriate level and method of monitoring, the Company applies a risk-based approach and considers:

- the size, nature, and complexity of the Company's operations;
- the overall ML/TF risk exposure associated with its business model;
- the effectiveness of internal systems, controls, and monitoring tools;
- existing internal procedures and controls implemented for operational and compliance purposes;
- the nature of products and services offered, including delivery channels and methods of communication (e.g., online onboarding, remote transactions, API integrations).

The Company ensures that monitoring systems and controls are proportionate, scalable, and capable of detecting suspicious activity in a timely manner, in line with applicable regulatory expectations and industry best practices.

Transaction Monitoring Measures

Measures applied by the Company for the ongoing monitoring of established business relationships are divided into two main categories: real-time screening and post-transaction monitoring.

Screening (Real-Time Monitoring)

The Company performs real-time transaction monitoring based on predefined parameters, scenarios, and risk indicators derived from the customer's profile, transaction behavior, and regulatory typologies.

Screening measures may be applied prior to, during, or immediately after the execution of a transaction and may result in the following actions:

- temporary suspension or rejection of a transaction;
- application of Enhanced Due Diligence (EDD) measures, including verification of source of funds (SoF) and purpose of the transaction;
- reassessment and, where necessary, adjustment of the customer's risk profile;
- escalation and submission of an internal report to the Compliance Officer for further review;
- submission of external reports to competent authorities (e.g., Financial Intelligence Units such as FINTRAC or relevant EU FIUs), where suspicion is confirmed.

Escalation and Decision-Making Framework

All alerts generated by the transaction monitoring system are subject to risk-based review by the Compliance function. The Company ensures that:

- alerts are reviewed within defined timeframes based on risk severity;

- decision-making is documented and auditable;
- suspicious activity is escalated without delay;
- reporting obligations are fulfilled in accordance with applicable AML/CTF regulations.

Post-Transaction Monitoring

The Company performs post-transaction monitoring, which involves the analysis of transactions after their execution in order to identify suspicious activity or circumstances that may not have been detected during real-time screening.

This includes transactions that, due to their nature, structure, or timing, did not initially trigger predefined monitoring scenarios or thresholds.

Post-transaction monitoring measures may result in the following actions:

- temporary or permanent account suspension;
- application of Enhanced Due Diligence (EDD), including verification of source of funds (SoF) and purpose of transactions;
- reassessment and update of the customer's risk profile;
- escalation and submission of internal reports to the Compliance Officer;
- submission of suspicious activity reports (SARs/STRs) to the relevant Financial Intelligence Unit (FIU), as required by applicable laws and regulations.

In both real-time screening and post-transaction monitoring, the Company utilizes a combination of internal systems and third-party technological solutions. The Company also ensures that appropriately trained personnel are responsible for monitoring activities in accordance with established internal procedures.

Suspicious Transaction Indicators

When establishing and maintaining monitoring procedures, the Company takes into account guidance issued by competent authorities (including FINTRAC, FATF, and relevant EU regulatory bodies), as well as internal risk assessments.

The following are examples of indicators that may be associated with suspicious activity:

- large or unusually frequent deposits or withdrawals;
- transaction patterns inconsistent with the customer's known profile or expected activity, including:
    - use of an account as a temporary repository for funds;
    - periods of inactivity followed by sudden spikes in transaction volume;
- structuring (smurfing), i.e., multiple smaller transactions conducted to avoid reporting thresholds;
- circular or "U-turn" transactions, where funds are transferred between parties and returned to the originator;
- repeated transactions just below regulatory or internal thresholds;
- excessive transfers involving multiple counterparties without clear economic rationale;
- involvement of intermediaries, shell entities, or complex ownership structures without a legitimate business purpose;
- transactions involving high-risk jurisdictions or sanctioned regions.

Use of Technology and Human Oversight

- The Company ensures that transaction monitoring is supported by appropriate automated systems capable of detecting suspicious patterns, while also maintaining human oversight to review alerts, apply judgment, and make final determinations.
- All monitoring activities are documented, auditable, and subject to periodic review to ensure effectiveness and compliance with regulatory expectations.

Additional Suspicious Activity Indicators

The Company considers a range of additional indicators that may signal elevated ML/TF risk, including but not limited to:

- involvement of shelf or shell companies with no clear economic purpose;
- entities incorporated in jurisdictions commonly associated with offshore financial centers or tax havens;
- use of corporate service providers, formation agents, or nominee arrangements acting as authorized signatories without transparent ownership structure;
- customers operating as money service businesses, gambling operators, or other high-risk sectors without sufficient transparency or regulatory clarity.

The following behavioral indicators are also taken into account:

- refusal or unwillingness to provide information or documentation required to verify the customer's identity, beneficial ownership, or business activity;
- provision of documents or information that appear false, inconsistent, or unreliable;
- refusal or inability to provide information necessary for ongoing monitoring (e.g., source of wealth/funds, purpose of transactions);
- customer activity that is inconsistent with the expected profile, declared business activity, or known financial position.

Transaction-Based Risk Indicators

The Company also pays particular attention to transaction-related red flags, including:

- transactions involving virtual asset addresses or wallets linked (directly or indirectly) to high-risk sources, including darknet marketplaces, mixing/tumbling services, illegal gambling platforms, ransomware activities, or reported theft;
- flows of funds to or from jurisdictions associated with higher ML/TF risks, including countries with weak AML regimes, high levels of corruption, or subject to sanctions;
- excessive or unexplained cross-border transfers without clear economic rationale.

High-Risk Customer Categories

Enhanced scrutiny is applied where customers fall within higher-risk categories, including:

- politically exposed persons (PEPs), as well as their family members and close associates;
- customers linked to jurisdictions or activities associated with terrorism financing, organized crime, or other serious criminal activities.

Assessment and Reporting

The identification of one or more indicators does not automatically qualify a transaction or relationship as suspicious. All alerts and indicators are assessed in context, taking into account the full customer profile, transaction history, and supporting information.

Where suspicion is confirmed, the Company fulfills its legal obligations by submitting reports to the relevant Financial Intelligence Unit (FIU) in accordance with applicable AML/CTF regulations.

Use of External Guidance and Internal Frameworks

The Company maintains and regularly updates a comprehensive list of ML/TF risk indicators, including virtual asset-related risks and terrorist financing indicators, in a separate internal document (e.g., AML Risk Indicators Annex).

This framework is based on guidance issued by competent authorities (including FINTRAC, FATF, and EU regulatory bodies), as well as internal risk assessments and industry best practices.

Sanctions Policy

In addition to its AML/CTF framework, the Company implements a comprehensive sanctions compliance program to ensure adherence to all applicable international and local sanctions regimes.

The Company follows guidance issued by relevant authorities (including FATF, FINTRAC, EU authorities, and OFAC where applicable) and ensures compliance with legally binding sanctions requirements in all jurisdictions where it operates or conducts business.

The Company maintains the ability to identify sanctioned individuals, entities, and transactions that may arise in the course of its activities. At a minimum, the following sanctions regimes are taken into account:

- United Nations (UN) Sanctions;
- European Union (EU) Sanctions;
- Canadian Sanctions (including SEMA and related regulations);
- U.S. OFAC Sanctions (as a global best practice, where relevant);
- other applicable national or international restrictive measures.

The Company reserves the right to apply additional sanctions regimes or internal restrictions based on the decision of the Compliance Officer and the Company's risk appetite.

Sanctions Screening Procedure

The Company verifies whether a customer, beneficial owner, or related party is subject to sanctions as part of the onboarding process and on an ongoing basis throughout the business relationship.

To prevent the establishment of business relationships or execution of transactions involving sanctioned parties, the Company implements an effective and risk-based screening framework, which includes:

- screening customers, beneficial owners, directors, and authorized persons against relevant sanctions lists at onboarding;
- ongoing screening of customers and related parties against updated sanctions lists on a real-time or near real-time basis;
- re-screening of the customer base upon updates to sanctions lists;
- screening of transactions to identify direct or indirect links to sanctioned individuals, entities, or jurisdictions;
- where applicable, screening of virtual asset wallets using blockchain analytics tools to identify exposure to sanctioned addresses.

Escalation and Handling of Sanctions Matches

All potential sanctions matches (hits) are subject to review and validation by the Compliance function. The Company distinguishes between false positives and confirmed matches using a risk-based assessment.

Where a sanctions match is confirmed, the Company will:

- immediately block or reject the transaction;
- freeze the relevant account or assets, where required by law;
- terminate or restrict the business relationship where applicable;
- report to the competent authority in accordance with legal obligations.

Controls and Governance

The Company ensures that:

- sanctions screening tools are regularly updated and calibrated;
- staff are trained to identify and escalate potential sanctions risks;
- all decisions related to sanctions are documented and auditable;
- internal controls are periodically reviewed to ensure effectiveness.

Sanctions Identification and Matching Process

To verify whether a person identified through screening corresponds to an individual or entity listed under applicable sanctions regimes, the Company uses all available identifying data.

For legal entities, this includes (where available):

- legal name and trade name;

- registration number and jurisdiction of incorporation;
- date of incorporation;

For natural persons, this includes:

- full name;
- date of birth;
- nationality and other identifying information.

The Company applies a risk-based matching methodology, taking into account potential variations in data, including:

- transliteration of names across different alphabets;
- alternative spelling or ordering of names;
- use or omission of diacritics;
- minor discrepancies in identifying details.

All potential matches are analyzed to distinguish true matches from false positives, using a combination of automated tools and manual review by the Compliance function.

Escalation of Potential Matches

If a potential sanctions match is identified, or if there is reasonable suspicion that a person may be subject to sanctions, the case must be immediately escalated to the Compliance Officer.

The Compliance Officer is responsible for:

- conducting further analysis and verification;
- requesting additional information or documentation where necessary;
- determining whether the match is confirmed or a false positive.

Actions upon Identification of a Sanctioned Person or Transaction

If the Company determines that a customer, beneficial owner, or counterparty is subject to sanctions, or that a transaction violates applicable sanctions regimes, the Company shall take immediate action in accordance with applicable laws and internal policies.

Such actions include:

- refusal to establish a business relationship or execute a transaction;
- immediate suspension or blocking of the transaction;
- freezing of assets, where required by applicable sanctions legislation;
- termination of the business relationship, where appropriate;
- reporting to the relevant competent authority (e.g., Financial Intelligence Unit or sanctions authority) without delay.

The Company applies a strict zero-tolerance approach to sanctions breaches and does not engage in business relationships involving sanctioned individuals, entities, or jurisdictions.

Regulatory Communication and Follow-Up

Following the identification of a confirmed sanctions match, the Company:

- submits required reports to the competent authority in accordance with legal obligations;
- maintains all relevant records and documentation;
- cooperates fully with regulatory authorities;
- follows any further instructions or requirements issued by the competent authority.

Reporting

Internal Reporting

The Company maintains a formal internal reporting framework to ensure timely escalation of any knowledge or suspicion of money laundering, terrorist financing, or sanctions breaches.

All employees are under a legal and regulatory obligation to promptly report to the Compliance Officer where they:

- know or suspect that a transaction or activity may be related to money laundering, terrorist financing, or sanctions violations;
- have reasonable grounds to suspect that a person is engaged in financial crime.

This obligation applies not only in cases of actual knowledge or suspicion, but also where an employee ought reasonably to have formed such suspicion based on the available information.

Reporting Procedure

Employees must submit an internal report to the Compliance Officer without undue delay and in any event within a defined timeframe (e.g., within 24 hours of forming suspicion).

Internal reports:

- must be submitted in a standardized format approved by the Company;
- must contain all relevant information and supporting documentation available at the time;
- must be treated as strictly confidential.

Where appropriate, the Company may delay or suspend a transaction pending internal review, to the extent permitted by applicable law.

Role of the Compliance Officer

Upon receipt of an internal report, the Compliance Officer shall:

- promptly assess the information provided;
- determine whether the suspicion is substantiated;
- request additional information where necessary;
- ensure proper documentation and record-keeping of the case.

External Reporting and Escalation

Where suspicion is confirmed, the Company shall submit a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) to the relevant Financial Intelligence Unit (FIU) or competent authority, in accordance with applicable legal and regulatory requirements.

The Company ensures that:

- reporting is conducted without delay;
- tipping-off prohibitions are strictly observed;
- all communications with authorities are properly documented.

Controls and Safeguards

The Company ensures that:

- employees are regularly trained on identifying and reporting suspicious activity;
- reporting channels are clear, accessible, and confidential;
- internal reports are handled independently and objectively;
- all reporting processes are auditable and subject to periodic review.

External Reporting Submission Methods

The Company ensures that all external reporting to competent authorities is conducted through secure, encrypted channels that guarantee the confidentiality, integrity, and protection of transmitted data.

Depending on the regulatory requirements and technical capabilities, the Company may use the following reporting methods:

- web-based reporting (manual submission);
- batch reporting (bulk file submission);
- API-based reporting (automated integration).

Web-Based Reporting

Web-based reporting enables the manual submission of individual reports via the relevant authority's secure reporting portal.

The system typically includes built-in validation controls to identify incomplete or incorrectly formatted data. The Company ensures that:

- all mandatory fields are completed accurately;
- any validation errors are promptly corrected prior to submission;
- submitted reports are reviewed for completeness and accuracy.

This method is typically used for submitting individual reports such as:

- Suspicious Activity Reports (SARs) / Suspicious Transaction Reports (STRs);
- regulatory threshold-based reports (where applicable);
- other ad hoc regulatory notifications.

Batch Reporting

Batch reporting allows the submission of multiple reports simultaneously through structured data files formatted in accordance with the technical specifications of the relevant authority.

The Company ensures that:

- all batch files comply with prescribed data formats and validation rules;
- files are pre-validated prior to submission;
- any rejected files are corrected and resubmitted without delay;
- accepted files are subject to internal review for accuracy and completeness.

Batch reporting is typically used for:

- high-volume transaction reporting;
- periodic regulatory reporting obligations.

API-Based Reporting

Where available, the Company may implement API-based reporting solutions to enable automated, real-time or near real-time submission of reports to competent authorities.

Such integrations are designed to:

- minimize manual intervention;
- reduce the risk of human error;
- ensure timely reporting in line with regulatory deadlines.

Governance and Controls

The Company ensures that all reporting methods are subject to appropriate internal controls, including:

- restricted access to reporting systems;
- audit trails for all submitted reports;
- periodic testing and validation of reporting processes;
- alignment with applicable data protection and confidentiality requirements.

All external reporting is conducted in accordance with applicable legal and regulatory obligations and under the oversight of the Compliance Officer.

Technical Requirements for External Reporting

To ensure secure and compliant external reporting, the Company implements appropriate technical and organizational measures in line with the requirements of competent authorities.

Where batch reporting is used, the Company ensures that:

- appropriate reporting software or secure transmission tools are implemented;
- access to reporting systems is properly configured and restricted;
- encryption and secure transmission protocols are applied;
- authentication mechanisms (e.g., credentials, certificates, or API keys) are in place.

Where required, the Company obtains and maintains necessary digital certificates (e.g., Public Key Infrastructure (PKI)) or equivalent authentication tools to enable secure communication with reporting systems.

API-Based Reporting Implementation

Where supported by the relevant authority, the Company may implement API-based reporting to enable automated, system-to-system submission of regulatory reports.

For API integration, the Company ensures that:

- secure authentication credentials (e.g., API keys, client secrets) are obtained and properly managed;
- reporting endpoints are configured in accordance with technical specifications provided by the authority;
- all submissions comply with applicable data validation and formatting rules;
- testing and validation procedures are completed prior to production use.

Fallback Reporting Methods

In exceptional circumstances where electronic reporting is not available or temporarily unavailable, the Company may use alternative submission methods permitted by the competent authority, including:

- manual submission through approved forms;
- other officially designated communication channels.

Such fallback methods are used only where necessary and in accordance with regulatory guidance.

Data Validation and Error Handling

The Company ensures that:

- all reports are validated prior to submission;
- errors or rejected submissions are promptly corrected and resubmitted;
- accepted submissions are subject to internal quality review;

- reporting processes include controls to prevent incomplete or inaccurate reporting.

Confidentiality and Security

All reporting processes are designed to ensure:

- confidentiality of sensitive data;
- integrity of transmitted information;
- protection against unauthorized access or disclosure.

Appropriate logging and audit trails are maintained for all reporting activities.

External Suspicious Transaction Reporting (STR/SAR)

Where the Company knows, suspects, or has reasonable grounds to suspect that a transaction or attempted transaction is related to money laundering, terrorist financing, or other financial crime, it shall take appropriate action without delay.

This includes, where permitted by applicable law:

- suspending or delaying the execution of the transaction;
- refraining from processing the transaction;
- initiating an internal investigation and escalation process.

Such actions are taken irrespective of the transaction amount.

Assessment of Suspicion

Suspicious activity is identified and assessed through:

- transaction monitoring systems and screening processes;
- analysis of customer behavior and transaction patterns;
- evaluation of relevant facts, circumstances, and supporting information;
- application of internal ML/TF risk indicators and typologies.

The Company ensures that suspicion is based on a holistic assessment of the available information and not solely on a single indicator.

Reporting Obligation

Where suspicion is confirmed, the Company shall submit a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) to the relevant Financial Intelligence Unit (FIU) or competent authority, in accordance with applicable legal and regulatory requirements.

The report shall include:

- a clear description of the suspicious activity;
- relevant transaction details;
- the rationale for suspicion;
- any supporting documentation or contextual information.

Reports must be submitted as soon as practicable after suspicion is formed, and in line with regulatory timelines.

Timing and Execution Controls

Where suspicion arises prior to the completion of a transaction, the Company will, where legally permitted:

- delay or suspend the transaction pending review;
- ensure that no action is taken that could facilitate financial crime.

Where suspicion arises after execution, the Company will:

- conduct a documented investigation;
- submit a report without delay;
- consider additional risk mitigation measures (e.g., account restrictions, enhanced monitoring, or termination of the relationship).

Governance and Record-Keeping

The Compliance Officer is responsible for:

- reviewing and approving all external reports;
- ensuring timely submission to the relevant authority;
- maintaining records of all internal investigations, decisions, and reports;
- ensuring auditability of the reporting process.

All investigations and reporting decisions are fully documented and retained in accordance with applicable record-keeping requirements.

Additional Considerations

- There is no minimum monetary threshold for suspicion-based reporting.
- Multiple related transactions may be included in a single report where appropriate.
- The Company strictly complies with tipping-off prohibitions and ensures confidentiality throughout the process.

Data retention

The Company must retain certain data and documents about its customers and transactions. Documents and data must be retained in a manner that allows for exhaustive and immediate response to the request from the Compliance Officer or for the response within 30 days to the request from FINTRAC or, pursuant to legislation, other supervisory authorities, investigation authorities or the court.

The Company shall implement all rules of protection of personal data upon the requirements arising from the applicable legislation. The Company is allowed to process personal data gathered upon CDD measures implementation only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

Record keeping

The Company shall keep (complete) the following electronic or machine-readable records reflecting monetary operations and transactions (hereinafter – records):

- record about the customer and business relationship
- record of every report sent to FINTRAC
- record of large cash or virtual currency transactions of $10,000 or more
- record of any transactions of $3,000 or more
- record of EFT or transmission of funds by other means of $1,000 or more
- record of virtual currency transfers equivalent to $1,000 or more
- record of foreign currency exchange or virtual currency exchange transaction tickets
- record of services provided by crowdfunding platform
- record of service agreements and internal memorandums about the provision of services

Record Storage and Data Management

All records relating to customers, transactions, and business relationships shall be entered into the Company's internal systems in a timely manner and maintained in chronological order.

Records shall be based on reliable and legally valid source documents evidencing the execution of transactions, monetary operations, or related activities. Such records must be created immediately or as soon as reasonably practicable following the execution of a transaction or operation.

The Company ensures that all record-keeping processes are centralized, consistent, and supported by internal systems designed to:

- maintain data integrity and prevent unauthorized modification;
- ensure full auditability of all entries and changes;
- enable efficient retrieval and reconstruction of customer activity;
- support internal monitoring, compliance review, and regulatory reporting.

All records shall be stored in electronic form within the Company's internal systems. The Company shall ensure that:

- data is securely stored and protected against unauthorized access, loss, or destruction;
- appropriate backup and recovery mechanisms are in place;
- records can be exported in a readable format (e.g., Excel, Word, or equivalent formats) without compromising data integrity;
- access to records is restricted based on role and business need.

Data Retention Periods

The Company shall retain all data and documentation relating to customers, transactions, reports, and business relationships for a minimum period of five (5) years, calculated from the latest of the following events:

- execution of the relevant transaction or monetary operation;

- submission of a report to a competent authority;
- termination of the business relationship with the customer;
- completion of contractual obligations.

Where required by applicable law, regulatory requirements, or instructions from competent authorities, retention periods may be extended. Under no circumstances shall records be retained for a shorter period than required by applicable legislation.

The Company ensures that retained data remains accurate, accessible, and usable throughout the entire retention period.

Upon expiry of the applicable retention period, data shall be securely deleted or anonymized, unless:

- further retention is required by law;
- an investigation, audit, or regulatory request is ongoing;
- a competent authority instructs the Company to retain such data for a longer period.

Staff Training and Awareness

The Company maintains a structured AML/CTF training program to ensure that all employees, agents, and other authorized representatives possess the knowledge and competencies necessary to perform their duties in compliance with applicable AML/CTF requirements.

All personnel involved in the Company's operations are required to:

- understand their responsibilities under the AML/CTF framework;
- be able to identify potential indicators of money laundering, terrorist financing, and sanctions evasion;
- follow internal procedures for escalation and reporting.

As part of the onboarding process, the Company verifies that employees possess appropriate qualifications, experience, and professional competence relevant to their roles.

The Company provides ongoing training on a regular basis, which is:

- risk-based and tailored to the employee's function;
- updated to reflect regulatory developments and emerging risks;
- documented and subject to internal review.

Additional targeted training is provided to employees in higher-risk roles, including those involved in onboarding, transaction monitoring, compliance, and reporting.

The Company maintains records of all training activities to demonstrate compliance with regulatory expectations and to support internal and external audits.

The responsibility for overseeing data retention and deletion processes lies with the Compliance Officer, who ensures that such processes are properly documented, controlled, and auditable.

Additional Training Governance and Effectiveness Measures

The Company ensures that its AML/CTF training program is not only formally implemented but also effective in practice. For this purpose, the Company applies the following additional controls:

All employees, agents, and relevant third parties are required to complete mandatory AML/CTF training:

- upon onboarding (prior to performing regulated functions); and
- on a periodic basis, at least annually or more frequently where required by risk level or regulatory developments.

Training programs are tailored to the specific roles and responsibilities of employees. In particular, enhanced and more specialized training is provided to:

- employees involved in customer onboarding and KYC processes;
- staff responsible for transaction monitoring and investigations;

- compliance personnel and senior management;
- employees involved in payment operations, virtual currency activities, or high-risk products.

The Company ensures that training covers not only general AML/CTF principles but also:

- sanctions compliance and sanctions evasion risks;
- fraud typologies and emerging financial crime risks;
- transaction monitoring scenarios and red flags;
- risks related to virtual assets and cross-border transactions.

To ensure effectiveness, the Company implements knowledge assessment mechanisms, which may include:

- testing or evaluation following training sessions;
- scenario-based exercises;
- periodic reassessment of employee understanding.

The results of such assessments are documented and may be used to identify knowledge gaps and improve the training program.

The Compliance Officer is responsible for:

- overseeing the development and implementation of the training program;
- ensuring that training materials remain up to date;
- maintaining records evidencing completion of training;
- periodically reviewing the effectiveness of the training framework.

The Company maintains a complete audit trail of all training activities, including:

- training materials used;
- dates of training sessions;
- list of participants;

- assessment results (where applicable).

Training effectiveness is periodically reviewed as part of the Company's overall AML/CTF compliance review and internal audit process.

Review of the Compliance Program

The Company ensures that the effectiveness of its AML/CTF compliance program is subject to regular, independent, and risk-based review (the "Effectiveness Review") in order to assess whether the program is adequately designed, properly implemented, and functioning effectively in practice.

The Effectiveness Review shall be conducted by an auditor or reviewer who possesses appropriate qualifications, expertise, and experience in AML/CTF and financial crime risk management. The reviewer must have unrestricted access to all relevant information, systems, and personnel across the Company.

To ensure objectivity, the person conducting the review shall be independent from the day-to-day execution of AML/CTF controls. Where an external auditor is not engaged, the Company shall ensure that the reviewer is not directly involved in operational AML/CTF activities and is able to perform the review objectively.

The Effectiveness Review shall be conducted at least annually or more frequently where required based on the Company's risk profile, regulatory expectations, or material changes in business activities.

The scope of the Effectiveness Review shall cover, at a minimum:

- the Company's AML/CTF policies and procedures;
- the risk assessment framework and its practical application;
- the customer onboarding and due diligence processes;
- the transaction monitoring and escalation framework;
- sanctions screening and controls;

- suspicious transaction reporting procedures;
- the training program and staff awareness.

The review shall include not only a formal assessment of documentation but also testing of the effectiveness of controls in practice. Such testing may include:

- interviews with relevant employees involved in onboarding, transaction monitoring, and compliance;
- detailed review of policies, procedures, and internal documentation;
- sampling and testing of customer files, including high-risk relationships;
- review of transaction monitoring alerts and investigation outcomes;
- assessment of reporting practices, including suspicious transaction reporting;
- evaluation of sanctions screening and escalation processes.

The depth and extent of the review shall be proportionate to the Company's size, complexity, nature of services, and level of financial crime risk exposure.

The results of the Effectiveness Review shall be documented in a formal written report (the "Review Data"), which shall include:

- identified deficiencies and weaknesses;
- recommendations for improvement;
- agreed remediation actions and timelines;
- assessment of the overall effectiveness of the AML/CTF framework.

The Review Data shall be submitted to the Compliance Officer and Senior Management. Where significant deficiencies are identified, the results shall be escalated to the Board of Directors or equivalent governing body.

The Company shall establish a structured remediation process to address findings identified during the review. This includes assigning responsibility for corrective actions, setting implementation deadlines, and monitoring progress. Follow-up reviews shall be conducted where necessary to confirm that deficiencies have been properly addressed.

All Review Data shall be:

- documented in a clear and structured format;
- retained for a minimum of five (5) years;
- stored securely and separately from operational data;
- accessible for internal audit and regulatory review purposes.

Access to Review Data shall be restricted to authorized personnel and shall not be disclosed without appropriate approval, unless required by law or regulatory authority.

The Review Data shall be maintained in chronological order and in a format that allows for effective analysis and linkage to other relevant compliance and operational data.

The reviewer shall submit the final report within a reasonable timeframe following completion of the review (typically within 30 days), including:

- detailed findings and recommendations;
- updates made during the reporting period;
- status of previously identified issues and remediation measures.

Annexes

Annex 1. Resolution Approving the AML/CTF Compliance Program - The Company's formal resolution approving the AML/CTF Compliance Program, including confirmation of management responsibility and oversight.

Annex 2. Services Description - Description of the services provided by the Company, including business model, customer types, delivery channels, and geographic exposure.

Annex 3. Enterprise-Wide Risk Assessment (EWRA) - Comprehensive assessment of ML/TF risks at the Company level, covering customers, products, services, delivery channels, and jurisdictions.

Annex 4. Customer Risk Scoring Methodology - Detailed methodology for assigning customer risk levels, including scoring criteria, weighting, and thresholds for low, medium, and high-risk classifications.

Annex 5. Customer Risk Assessment Template - Standard template used for documenting individual customer risk assessments.

Annex 6. Customer Onboarding Procedure - Step-by-step procedure for customer onboarding, including identification, verification, and risk classification.

Annex 7. KYC / Identification Requirements Matrix - List of required documents and verification methods depending on customer type, risk level, and jurisdiction.

Annex 8. Beneficial Owner Identification Guidelines - Guidance on identifying and verifying ultimate beneficial owners (UBOs), including ownership thresholds and control considerations.

Annex 9. Source of Funds and Source of Wealth Procedure - Rules and procedures for assessing and verifying the legitimacy of customer funds and overall wealth.

Annex 10. Politically Exposed Persons (PEP) Procedure - Procedures for identifying, approving, and monitoring PEPs, their family members, and close associates.

Annex 11. Sanctions Screening Procedure - Procedures for screening customers and transactions against applicable sanctions lists (EU, UN, OFAC, UK), including handling of potential matches.

Annex 12. Transaction Monitoring Rules and Scenarios - Description of monitoring logic, risk indicators, thresholds, and scenarios used to detect suspicious activity.

Annex 13. Indicators of Suspicious Activities and Transactions (Red Flags) - List of behavioral and transactional indicators that may signal ML/TF or other financial crime risks.

Annex 14. Internal Reporting Form - Standard form used by employees to report suspicious activity to the Compliance Officer.

Annex 15. Suspicious Activity Reporting Procedure - Procedure for assessing, documenting, and submitting suspicious activity reports (SAR/STR) to competent authorities.

Annex 16. Ongoing Monitoring Procedure - Procedures for periodic review of customer profiles, risk re-assessment, and ongoing due diligence.

Annex 17. Record Keeping and Data Retention Rules - Detailed requirements for storing, retaining, and securely deleting AML/CTF-related data in compliance with applicable laws (including GDPR considerations).

Annex 18. Outsourcing and Third-Party Risk Management Policy - Framework for managing risks associated with outsourcing AML/CTF functions or relying on third parties.

Annex 19. IT Systems and Data Integrity Controls - Description of systems used for AML/CTF compliance, including data protection, audit trails, and system integrity controls.

Annex 20. AML/CTF Training Plan - Structured training program covering training scope, frequency, and target groups.

Annex 21. Training Records Template (Training Protocol) - Template for documenting completed training, including participants, content, and dates.

Annex 22. AML/CTF Governance and Escalation Matrix - Description of roles, responsibilities, reporting lines, and escalation procedures within the AML/CTF framework.

Annex 23. AML/CTF Effectiveness Review Methodology - Methodology for conducting independent reviews of the AML/CTF program, including scope and testing approach.

Annex 24. Effectiveness Review Report Template - Template for documenting findings, deficiencies, and remediation actions following AML/CTF audits or reviews.

Version Control Table

23.03.2026	First Issue

Director:

AML & Compliance Officer: