AML / CTF Compliance Program

CHAMONIX FINANCIAL LTD.

Canada

March 2024

- This AML/CTF Compliance Program (Program) shall apply to all branches and subsidiaries of CHAMONIX FINANCIAL LTD. (Company).
- This Program consists of main file, which established general principles for certain procedures in the course of the Company's activity and annexes, which describe certain processes and/or requirements in details.
- Implementation of this Program will not detract from the obligation to comply with any other local law and is not to be regarded as enabling the implementation of acts that have been prohibited or restricted by local laws.
- The Company maintains full cooperation with law and regulatory authorities in legislations, investigations, and inquiries in Canada and abroad.
- This Program shall be accepted and approved by the resolution of the CEO and the Compliance Officer.

Administrative information

Company name: CHAMONIX FINANCIAL LTD.;

Registration number: BC1464886;

Address: 164-2223A OAK BAY AVENUE, MAILBOX #164,
VICTORIA BC V8R 0A4, CANADA;

Glossary

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	RBA Risk-Based Approach
RGS	Reasonable grounds to suspect
SoF	Source of Funds
SoW	Source of Wealth
TF	Terrorist Financing
UN	The United Nations
VASP	Virtual Asset Service Provider
VC	Virtual Currency
FE	Financial Entity
RE	Reporting Entity

Table of Contents

Introduction

The Company adopts appropriate, sufficient measures aimed to preventing its operations from being used as means to conceal, manage, invest, or use any form of money – or other assets – due to illicit activities, or to give the appearance of legality to such activities.

The company adopts a risk-based approach in the design and implementation of this Program with a view to managing and mitigating ML/TF risks. A qualified Compliance Officer has been appointed to implement appropriate AML/CTF policies and procedures.

Company's key AML/CTF Principles

In the course of its business activity, the Company implements the following principles:

- to comply with AML/CTF legislation in the countries in which it operates;
- to strive to fulfil international standards as detailed by the Financial Action Task Force (FATF) recommendations;
- to work in conjunction with FINTRAC and the governments of the countries the Company operates in, as well as support their objectives in relation to the prevention, detection and control of ML/TF;
- the Company may decide not to provide products or services based upon decisions guided by ML/TF risk appetite and corporate social responsibility;
- to comply with primary legislation of Canada on AML/CTF.

Company's Compliance Program

The Company has established this Program to ensure that any ML/TF risks identified by the Company are appropriately managed and mitigated. This means having adequate systems and controls in place to mitigate the risk of the Company being used to facilitate any financial crimes. This Program is designed to represent the basic standards of AML and CTF procedures and standards, which will be strictly observed by Company.

The Program is based upon applicable AML/CTF laws, regulations and regulatory guidance from the Government Institutions of Canada. This Program is further designed to comply with the Financial Action Task Force (FATF) Standards on combating money laundering and the financing of terrorism and proliferation.

Among other things, this Program:

- forms part of its wider compliance regime, and is designed to meet the requirements of its legislative environment;
- ensures that the Company is able to detect suspicious activities associated with money laundering, fraud, and terrorist financing, and report them to the appropriate authorities;
- focuses not only on the effectiveness of internal systems and controls developed to detect money laundering, but on the risk posed by the activities of customers with which Company does business;
- is built on a strong foundation of regulatory understanding and overseen by personnel who are experienced and knowledgeable enough to create a climate of compliance at every level of their organization.

Review of the Program

This Program is the subject of a review by the CEO and the Compliance Officer at least every two years. The proposal for a review and the review of this Program may be scheduled more often by the decision of the Company's Compliance Officer. The Company must review and, where necessary, update this Program and its annexes (incl. the risk assessment policy and risk assessment made thereof) in the each of the following cases:

- publication of the results of the National Money Laundering and Terrorist Financing Risk Assessment;
- upon receipt of an order from the FINTRAC strengthen the applicable internal procedures;
- upon significant events or changes in the Company's management and operations;
- such necessity arises during periodic monitoring of the implementation and adequacy of the Company's internal policies.

This Program's review (incl. regular annual review) shall be confirmed with the relevant resolution signed by the CEO and the Compliance Officer.

Governance Principles

The Company's employees and the service providers (third parties) involved in the Company's activity should act in accordance with this Program. The obligations of the Company as defined in this Program must be understood as the duties of all employees of the Company unless it is provided that certain duties must be performed by a specially designated employee of the Company (e. g. the CEO, the Compliance Officer, etc.).

All employees of the Company, depending on the functions performed by them, shall be introduced to this Program. They should be aware of their subordination to other structural units of the Company. If the Company has more than 1 Employee in a structural unit, the CEO shall appoint a responsible employee whose task is, among other things, to perform daily supervision over the performance of the tasks of the structural unit (or part of it). The Company's CEO must ensure that all newly recruited employees are made aware of this Program and the Company's structure.

The day-to-day management of the Company takes place through the CEO. The CEO is responsible for assigning tasks to the Company's structural units and controlling the performance of tasks assigned. In case when the relevant Employee or third party is not appointed for performing of structural unit's functions, the CEO shall be responsible for this structural unit's functions. In addition to day-to-day management, the CEO organizes meetings and, if necessary, discusses decision-making with experts (incl. employees, advisors and external service providers).

Company's Services

The Company operates as a Money Service Business (MSB) as it is specified in Canadian legislation. The Company has developed services description (annex 2) as separate document, which establishes the following in regards of each service offered by the Company:

- conditions to be fulfilled for provision of the service;
- service provision flow, incl. possible assets flows.

Before offering new services or any changes in way of the services provision, the Company shall update services description document and assess risks related to such changes, including, but not limited to, risks which may affect the service users' anonymity.

All of the Company's services of virtual currency exchange operator are provided electronically [through email and website operated by the Company]

Money Laundering

The term "money laundering" (ML) means any act or attempted act to disguise the source of money or assets derived from criminal activity.

There are three common stages in ML, and they frequently involve numerous transactions. A VASP should be alert to any such sign for potential criminal activities. These stages are:

1) Placement – the physical disposal of assets proceeds derived from illegal activities;
2) Layering – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail, and provide anonymity; and
3) Integration – creating the impression of apparent legitimacy to criminally derived wealth. In situations when the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

- Illicit funds are physically placed in the financial institution

- Multiply transactions
- Wire transfers between domestic and foreign accounts

- Real estate investment
- Purchase of luxury assets
- Investments in Securities Markets

Terrorist Financing

The term "terrorist financing" (TF) means an offence within the meaning of Article 2 of the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999[1]. Article 2.1 defines the crime of terrorist financing as the offense committed by any person who by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out an act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex of International Convention for the Suppression of the Financing of Terrorism of 9 December 1999 or any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

Similar to money laundering, terrorist financing generally consists of three stages:

1) Raising – generating the funds intended for a terrorist or terror organization. The funds can originate from a variety of sources (incl. from illicit activity as well as legal business operations);
2) Moving – upon raising required amount of funds, the funds are moved to a place where they can be accessed and used by a terrorist or terror organization;
3) Using funds – some examples of the use of funds in terrorism include using it for the terrorist or terror organization to pay for weapons, material, equipment, overheads, media, messaging, training, and salaries.

Despite the different stages, the ways in which terrorist financing is done is similar and, in some cases, may be identical to the methods used for money laundering.

Terrorists or terrorist organizations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

[1] https://treaties.un.org/doc/db/terrorism/english-18-11.pdf

AML/CTF systems

Primary Legislation Governing AML/CTF in Canada

The Company shall comply with the rules and regulations set out in Proceeds of Crime (Money Laundering) and Terrorist Financing Act **(PCMLTFA)**[2]. In addition, the following legal acts are relevant to the Company's activity (non-exhaustive list):

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (SOR/2002-184; hereinafter – **PCMLTFR**)[3];
- Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (SOR/2001-317; hereinafter – **PCMLTFSTRR**)[4];
- Criminal Code (R.S.C., 1985, c. C-46)[5];
- Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (SOR/2001-360)[6];
- the Canadian Financial Intelligence Unit's general guidelines regarding measures against money laundering, terrorist financing and regarding implementation of Ministerial Directives[7].

Company firmly believes that a reputation for integrity and openness, both in its business model and in its management systems and procedures - are crucial to achievement of its commercial goals and plans, and also to the fulfilment of its corporate responsibilities. The Company is, therefore, committed to the highest standards of AML/CTF measures in its operations, and it adheres to both established and recommended international standards to prevent the use of its services for the above purposes.

[2] https://laws-lois.justice.gc.ca/eng/acts/P-24.501/
[3] https://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-184/
[4] https://lois-laws.justice.gc.ca/eng/regulations/SOR-2001-317/
[5] https://laws-lois.justice.gc.ca/eng/acts/c-46/
[6] https://laws-lois.justice.gc.ca/eng/regulations/sor-2001-360/
[7] https://fintrac-canafe.canada.ca/msb-esm/msb-eng

Ubuntu Light (Headings) Supervisory Authority

For the purpose of AML/CTF, MSBs and FMSBs registered are supervised by the state authority with the following details:

- The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC);
- registration number: 188608786;
- address: 234 Laurier Avenue West, 24th floor, Ottawa ON K1P 1H7, Canada;
- phone: +1-866-346-8722;
- email: communications3@fintrac-canafe.gc.ca.

The same authority examines the implementation of compliance program and receives, collects, and analyses financial transaction reports sent by the entities that are required by law to send reports. In addition, FINTRAC performs supervision under implementation of international and domestic sanction regimes.

Effective Controls

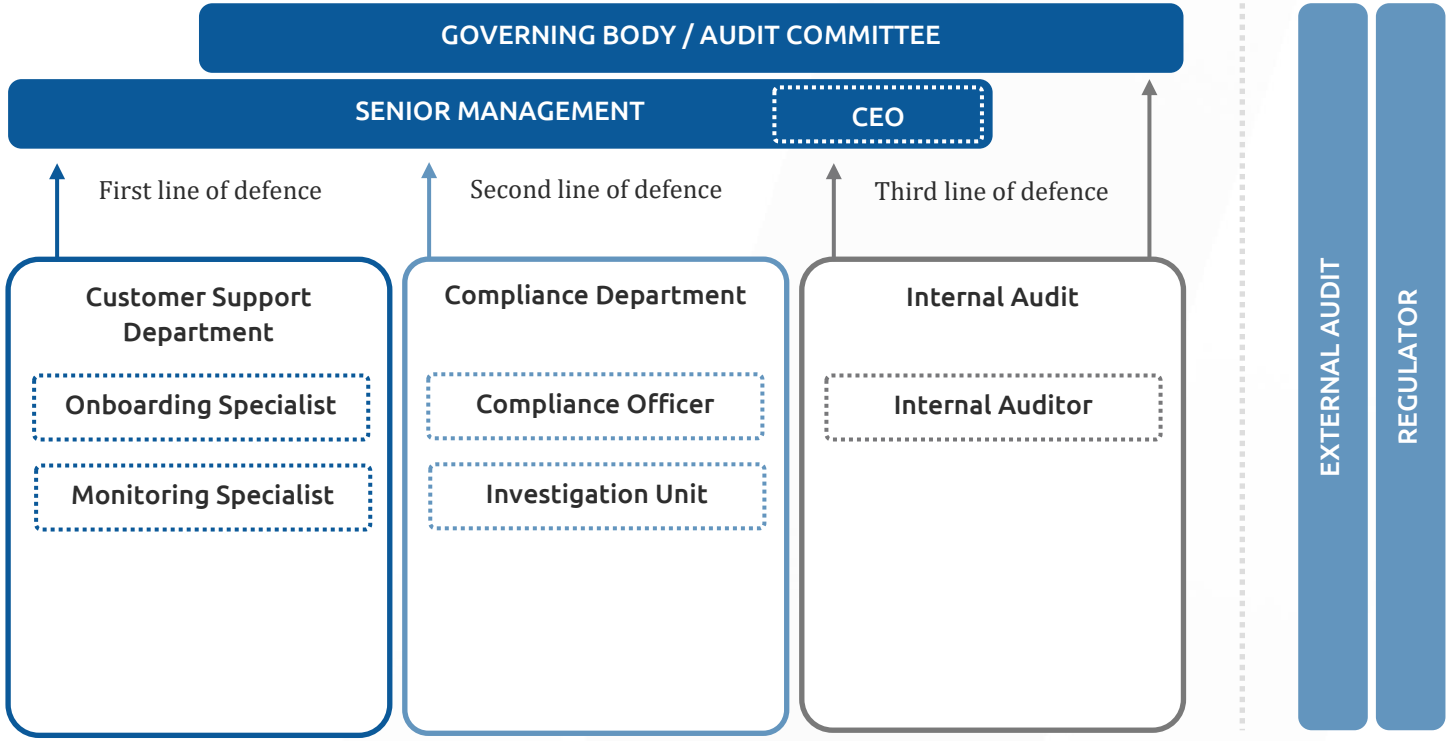
To ensure proper implementation of AML/CTF procedures and controls, Company has effective controls covering:

- effective AML/CTF compliance program
- senior management oversight
- appointment of the Compliance Officer and other employees with certain responsibilities;
- compliance and audit function;
- staff training.

The CEO of the Company is responsible for managing the business effectively and for the oversight of internal AML/CTF controls and systems. The CEO appoints the Compliance Officer who has overall responsibility for the establishment and maintenance of the Company' AML/CTF systems and is the central reference point for suspicious transaction reporting.

Three Lines of Defence

The Company follows the three lines of defence framework when managing ML/TF risks. The three lines of defence is an industry model for managing risk. It is used to structure roles, responsibilities and accountabilities for decision making, risk and control management, and independent assurance. The three lines of defence are used as the fundamental guiding principle when performing the AML/CTF obligations.



Senior Management Responsibilities

The Company's CEO is responsible for all Senior Management functions. The Company's Senior Management responsibilities include but are not limited to:

- maintaining compliance with effective laws of Canada
- monitoring and overseeing the compliance activities of the Company to ensure they are in accordance with the applicable laws, regulations and internal policies and procedures;
- reviewing the AML/CTF Compliance Program to ensure it is comprehensive, adequate and viable;
- approving the AML/CTF Compliance Program;
- ensuring that the AML/CTF Compliance Program is effectively implemented by the Company's Compliance Officer and other employees;
- designating a qualified employee to serve as the Company's Compliance Officer;
- reviewing the performance of the Compliance Officer;
- ensuring that the Compliance Officer has sufficient authority and resources (monetary, physical and personnel) to administer an effective AML/CTF Compliance Program based on the Company's risk profile;
- periodically receiving and reviewing reports presented by the Compliance Officer to ensure that the compliance program is being executed as approved and that it is, in fact, serving its intended purpose of maintaining the integrity, safety and soundness of the Company;
- annually reviewing changes proposed to be made to AML/CTF Compliance Program, and, if satisfied that the modifications are desirable, approving the modifications/changes;
- designating and contracting the services of a competent entity to perform independent compliance audits of the Company to test for the Company's level of adherence to the applicable AML/CTF laws and regulations.

The Senior Management of the Company have approved this AML/CTF Compliance Program and the designation of the Compliance Officer and have assigned responsibility to such person to maintain and monitor overall compliance on a day-to-day basis with AML/CTF requirements.

KYC Agents

KYC Agents comprise the first line of defence, which is a part of the risk management system that is related to the structural units with whose activities risks are associated and that must identify and assess these risks, their specific features and scope and that manage these risks by way of their ordinary activities, primarily by way of application of due diligence measures.

The first line of defence must have good knowledge of the customer and the specific features of their activities and business activities.

Principal functions of the KYC Agents include in particular:

- performing of the customer's onboarding procedure (as defined below) and application of CDD/EDD measures before the establishment of the Business Relationship with the customer;
- performing of the ODD/EDD measures in the course of the established Business Relationship with the customer (incl. the monitoring of transactions and periodically updating the customer's information);
- identifying transactions in the customer's activities that are suspicious or unusual or do not correspond to reasonable economic objectives, or transactions that refer to such circumstances, and referring such transactions to the second line of defence (Compliance Department) for analysis and if necessary, directly to the Senior Management;
- perform other functions which are assigned to the KYC Agents under the applicable law, internal policies, job description.

Compliance Department

Compliance Officer

The Compliance Officer acts as the focal point within the Company for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the Senior Management to ensure that ML/TF risks are adequately managed.

The Compliance Officer is sufficiently independent and has a direct reporting line to the Company's Senior Management. The Compliance Officer has access to sufficient resources and information to be able to ensure Company's compliance with effective laws and regulations of Canada.

In particular, the Compliance Officer assumes responsibility for:

- developing and/or continuously reviewing the AML/CTF systems (incl. risk assessment made thereof) to ensure they remain up-to-date and meet current statutory and regulatory requirements;
- the oversight of all aspects of the AML/CTF systems which include monitoring effectiveness and enhancing the controls and procedures where necessary.

The Compliance Officer plays an active role in the identification and reporting of suspicious transactions. Principal functions of the Compliance Officer include in particular:

- reviewing all internal disclosures and exception reports and determining whether or not it is necessary to make a report to the FINTRAC (incl. STR, LCTRs, LVCTRs, etc.);
- maintaining all records related to such internal reviews;
- providing guidance on how to avoid "tipping off" if any disclosure is made;
- acting as the main point of contact with the FINTRAC, law enforcement, and any other competent authorities in relation to ML/TF prevention and detection, investigation or compliance.

In addition, the Compliance Officer:

- organizes conducting of on-going monitoring of the Company's relationships with its customers and reviews of monitoring conducted on a regular basis;
- identifies suspicious transactions and activities;
- monitors changes of regulatory requirements with respect to ML/CTF prevention and counteraction; communicates all AML/CTF relevant issues to the Senior Management;
- develops internal training programs and materials, as well as receives relevant trainings.
- acts as a responsible person in the meaning of PCMLTFR appointed for implementing the Compliance Program;
- perform other functions which are assigned to the Compliance Officer under the applicable law, internal policies, job description.

Investigation Unit

Investigation Unit works under the auspice of the Compliance Officer. The following functions shall be performed by the Investigation Unit:

- assistance of the Compliance Officer regarding reviewing received internal disclosures and exception reports;
- assistance of the Compliance Officer regarding filing of reports to the FINTRAC;
- perform other functions which are assigned to the Investigation Unit under the internal policies and job description.

Audit Function

Audit function shall be established to perform regularly reviews of the AML/CTF systems to ensure their effectiveness. The frequency and extent of the review should be commensurate with the risks of ML/TF and the size of the Company's business, as well as regulatory requirements. Where appropriate, Company will seek a review from external auditors. Independent audit functions include the following principles:

- compliance and audit functions are independent in practice;
- the regular review is performed at a frequency of once a year;
- external party is leveraged to perform the auditing;
- availability of direct communication to Senior Management through regular committees (compliance committee) or other means of direct communication.

The performing of audit functions shall be ensured by the decision of Senior Management, which should be adopted, at least, on annual basis. The Senior Management may decide to avoid performing of audit for specific period, is such decision doesn't affect the Company's exposure to ML/TF risks and it is confirmed by the Compliance Officer. There's regulatory requirement to conduct audit at least every 2 years.

Risk-based approach (RBA)

By adopting a risk-based approach, the Company is able to ensure that measures to prevent or mitigate ML and TF threats are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

The inherent risk is assessed in the course of identification of the specific products, services, technologies, customers, entities, and geographic locations. Depending on the specific characteristics of the particular product, service, technologies or customer, the risks are not always the same. Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered.

Risk assessment during on-boarding stage of the new customer provides the Company with an opportunity to gain an insight into the type and nature of its potential customers, their geographic locations and business activities, whereas ongoing determination of the customer's risk profile allows the Company to ensure, that correct risk level is assigned to the customer throughout the established relationship.

The Company determines the extent of its CDD measures and ongoing monitoring, using a risk-based approach (RBA) depending upon the background of the customer and the product, transaction or service used by that customer, so that preventive or mitigating measures are commensurate to the risks identified.

The RBA enables the Company to subject its customers to proportionate controls and oversight by determining:

- the extent of the due diligence to be performed on the direct customer;
- the extent of the measures to be undertaken to verify the identity of any beneficial owner and any person purporting to act on behalf of the customer;
- the level of ongoing monitoring to be applied to the relationship;
- measures to mitigate any risks identified.

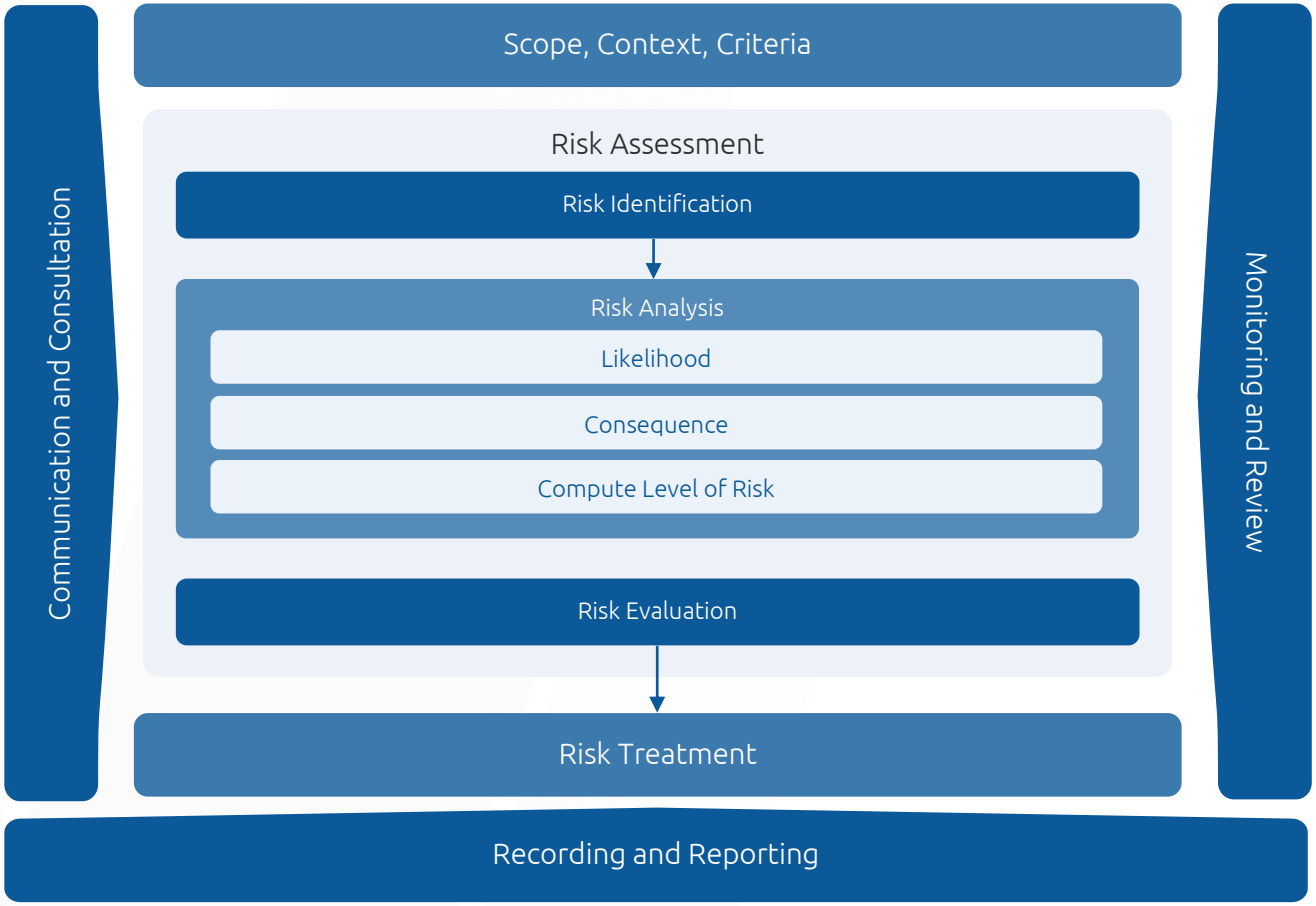
An RBA involves identifying and categorizing ML/TF risks at the customer level and establishing reasonable measures based on risks identified. An RBA does not refrain Company from engaging in transactions with customers or establishing business relationships with potential customers, but rather it assists Company to effectively manage potential ML/TF risks.

Risk Assessment and Risk Categories

The Company prepares and regularly updates the risk assessment in order to identify, assess, analyse and manage ML and TF risks. The process of risk assessment, executed by the Company shall include at least the following stages:

- risk factors identification;
- risks factors analysis;
- risks factors evaluation.

Risk assessment is an integral part of the risks management process within the RBA.



In the course of risk assessment, the Company uses at least the following sources:

- applicable regulatory requirements (Canadian laws, FINTRAC guidelines, etc.);
- last national risk assessment;
- guidelines of authorities (incl. international organizations, e. g. FATF);
- the knowledge previously obtained when performing activities similar to the Company.

The Company assess the ML/TF risks of its customers by assigning a ML/TF risk rating taking into consideration the risk categories as specified below.

Customer risk

Customer risk factors are related to the customer's or its beneficial owner's personality, their behaviour and other circumstances directly related to the specific person. Factors in this category include customer's legal status, its structure, information previously known about the customer, etc. When identifying risk factors in this category, the Company considers the following:

- the customer's status, such as entity listed on a regulated market, governmental authority or entity regulated by public law, credit or financial institution;
- the customer's PEP status, as well as known connection to PEPs (family members, close associates, etc.);
- complexity of the customer's organizational structure, including use of corporate structures, trusts and the use of nominee directors/shareholders and bearer shares;
- negative information about the customer or related persons (e. g. adverse media, warnings from regulatory bodies, criminal records, etc.);
- the customer's behaviour and personalities (e. g. education or knowledge in certain field, age, etc.);
- the customer's area of activity (e. g. cash intensive or other business vulnerable to ML or TF);
- origins of the customer's wealth and opportunities to verify their soundness.

Country or geographic region risk

Country or geographic region risk factors are related to specific jurisdiction or region. Factors in this category include the customer's citizenship, place of residence, location of business as well as location of transaction's counterparty (relevant country). When identifying risk factors in this category, the Company defines if the relevant country meets the following facts about jurisdiction and region:

- is the Company's domestic country;
- have been identified by the FATF as jurisdictions with strategic AML/CTF deficiencies;
- is subject to sanctions, embargoes or similar measures issued by Canada and/or UN;
- is vulnerable to corruption or other criminal activity;
- believed to have strong links to terrorist activities.

Product and/or services risk

Product and/or services risk factors are related to specific service being provided. Such factors include volume of services being provided to the customer, specific transactions patterns used and other circumstances, which may affect risk of ML/TF occurrence in the course of services provision. When identifying risk factors in this category, the Company considers the following facts about products and services:

- volume of products and/or services requested or provided;
- specific transactions patterns (e. g. FATF Red flags indicators);
- intended purpose of product and/or service, as well as identified purpose;
- product and/or service possible (and identified) use in activities vulnerable to ML or TF and in illicit (prohibited) activities;
- product and/or service ways to promote anonymity;
- product and/or service involvement in new developments and technologies.

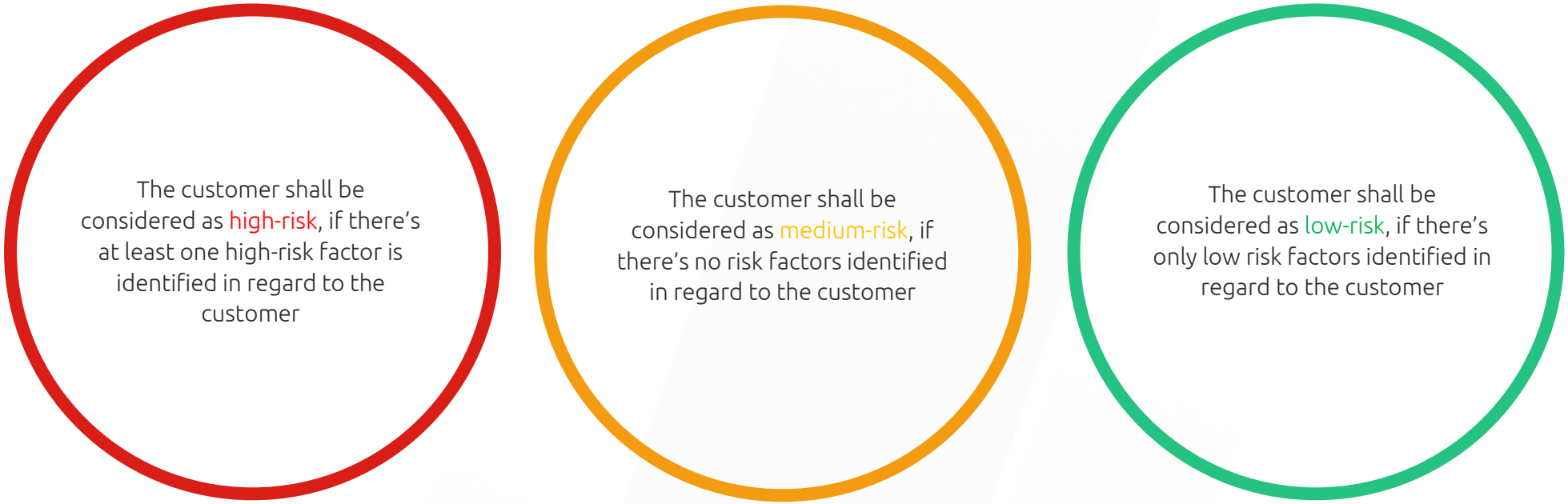
Delivery / distribution channel risk

Delivery and/or distribution channels risk factors are related to channels used for provision of the services. Such factors include specific ways for identity verification, performing transactions and authentication methods. When identifying risk factors in this category, the Company considers the following facts about delivery / distribution channel:

- the method using which the customer's and its representative's identity has been verified (e. g. via face-to-face meeting, remotely, by reliance to third party, etc.);
- credit institution, financial institution, paying institution or payment channel used by the customer;
- IP address(es) and device ID(s) used by the customer;
- use of solutions which promote anonymity by the customer (e. g. VPN, encrypted email, TOR browser, one-time wallets, etc.);
- new developments and technologies used in the course of product/service provision.

Determination of the customer's risk profile

The Company establishes and maintains the **list of risk factors** as separate document (annex 3), which is used for determination of the customer's risk profile.



The Company identifies risk factors in the course of customer due diligence as described below.

Maintaining of the customer's risk profile

The Company reviews the business relationship with each customer as per the schedule below to ensure if the risk profile determined is still applicable or should be modified based on any changes of the identity of the customer, the nature of the customer's business, the customer's

country of residence, the actual volume of transactions and other facts, which may affect the customer's risk assessment. Only the Compliance Officer is permitted to alter a customer's risk profile. The Compliance Officer will maintain relationship opening documentation, activity statements, and other necessary documentation to support the risk profiles assigned to customers.

Low Risk

The Compliance Officer will engage in annual reviews of each low-risk customer.

Medium Risk

The Compliance Officer performs annual reviews of every medium-risk customer that is no longer a new relationship (i. e. every 6 months after the customer's onboarding).

High Risk

Due to the high-risk nature of these relationships, the Compliance Officer performs monthly reviews of every high-risk customer including a transactional review.

Each high-risk customer will require Enhanced Due Diligence before the relationship and additional facts will be gathered to learn more about the customer. For any non-individual customer whose business has been identified as a "high-risk business", the Compliance Officer must also additionally verify the existence of the business and purpose of the business relationship with the Company.

Non-acceptable customers

The Company has created the list of prohibited risk factors (annex 3) in the presence of which the customer will not meet the Company's risk appetite. In case, when such risk factor has arisen in the course of the customer's onboarding or before making occasional transaction – the Company refuses to establish the business relationship or perform transaction with such customer. If prohibited risk factor is identified in the course of the business relationship established – such relationship shall be terminated in accordance with this Program.

Prohibition of anonymous accounts

The Company is prohibited from opening anonymous accounts or accounts under obviously fictitious names, as well as from opening accounts or otherwise starting business relationship without requesting data confirming the identity of the customer or if there is a reasonable suspicion that the data recorded in these documents is fake or falsified.

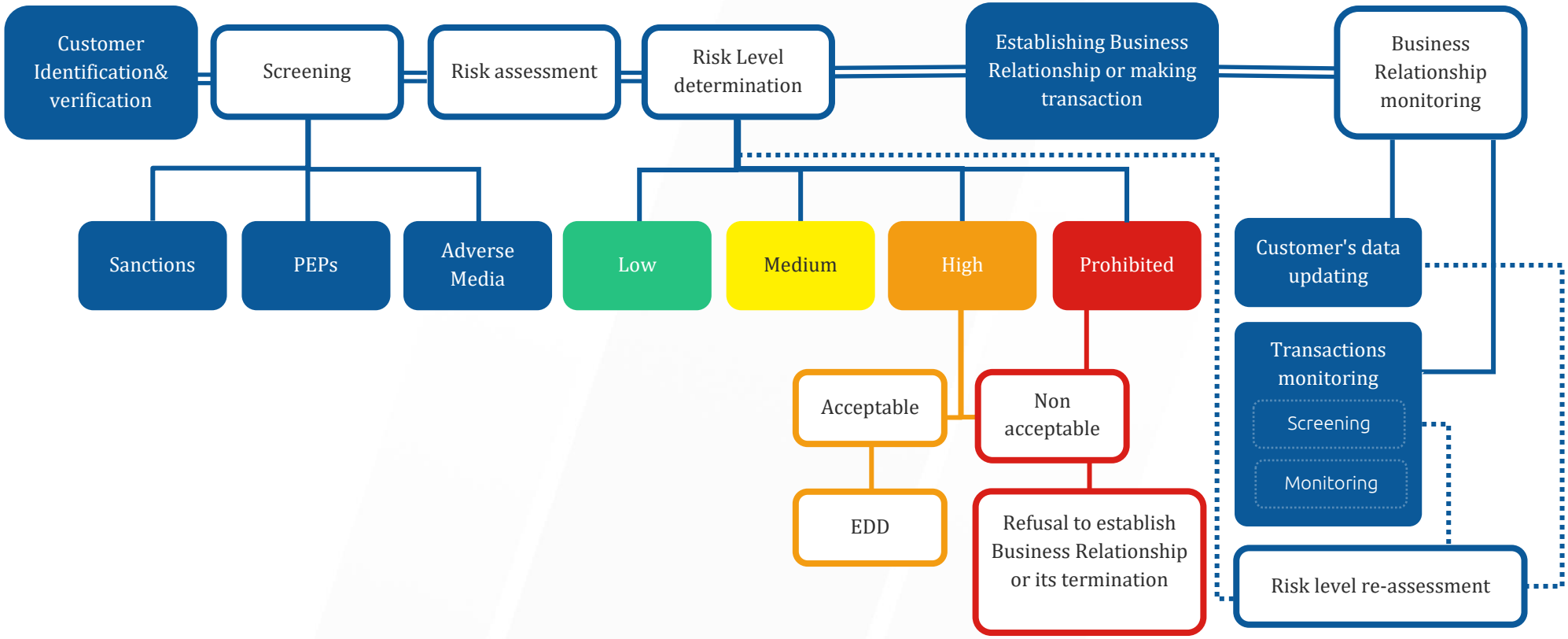
Prohibition of shell banks

The Company does not maintain correspondent relationships with shell banks, which is defined as a financial institution or an institution that carries out activities equivalent to those carried out by a financial institution, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, organizational structure and internal control systems, and which is unaffiliated with a financial group supervised by the competent authorities.

Customer due diligence

Customer due diligence (CDD) is central to an effective AML/CTF regime. The Company takes CDD measures to identify and verify each of its customers so it can:

- determine the money laundering and terrorism financing risk posed by each customer;
- decide whether to proceed with a business relationship or transaction;
- assess the level of future monitoring required.



The Company applies the following CDD measures:

- identification of the customer and verification of the customer's identity using prescribed methods to ensure accuracy of the information;
- identification and taking reasonable measures to verify the beneficial owner's identity so that Company is satisfied that it knows who the beneficial owner is, including in the case of a legal entity or trust, measures to enable Company to understand the ownership and control structure of the legal entity or trust;
- identification and taking reasonable measures to verify if the customer is a PEP/HIO or a person connected to PEP/HIO (family members, close associates, etc.);
- obtaining an information on the purpose and intended nature of the business relationship or transaction unless the purpose and intended nature are obvious;
- monitoring of the business relationship.

If a person purports to act on behalf of the customer, Company takes measures to:

- identify the person and take reasonable measures to verify the person's identity using reliable and independent source documents, data or information;
- verify the person's authority to act on behalf of the customer.

CDD measures should apply in the following cases:

- upon establishment of the business relationship;
- upon receiving of cash or virtual currency that exceeds $10,000[8] within 24 hours;
- when the person or entity conducts or attempts to conduct a suspicious transaction(s) , regardless of the value or exceptions provided for in this Program and applicable legislation, before sending a Suspicious Transaction Report (STR);
- upon issuing or redeeming any negotiable instruments (e.g., traveller's cheques, money orders, etc.) of $3,000 or more;

[8] References to dollar amounts are provided in Canadian dollars (CAD).

- upon transmitting $1,000 or more in funds by using an informal value transfer system (IVTS) for the currency exchange that works by transferring value without the need to physically transfer money, relying instead on personal connections between operators in different locations (e.g., Hawala remittance systems);
- upon initiating (i.e., transmission of instructions) an electronic funds transfer of $1,000 or more;
- upon an event of foreign currency exchange exceeding $3,000 or virtual currency exchange exceeding $1,000;
- upon executing or mediating virtual currency transaction(s) where the value of the transaction(s) exceeds $10,000;
- upon remitting funds that exceed $1,000 to a beneficiary by international funds transfer or virtual currency exceeding $1,000 by informal value transfer system;
- upon first creation of information record during the provision of crowdfunding platform services;
- upon an event of maintained crowdfunding platform donation that exceed $1000.

Timing of CDD

The Company completes the CDD process before the establishment of any business relationship for provision of services or conduction of occasional transaction(s) aforementioned.

The customer identification information (as well as information on any beneficial owners and PEP/HIO status) and information about the purpose and intended nature of the business relationship or transaction shall be obtained before entering into the business relationship or before completion of occasional transaction(s).

Where Company is unable to comply with relevant CDD requirements and the ongoing due diligence requirements, it must not establish a business relationship or carry out any occasional transaction with that customer or must terminate business relationship as soon as reasonably practicable (where applicable), and where there is relevant knowledge or suspicion, should send report to the FINTRAC.

Entering business relationship

The Company enters into a business relationship with a customer after the second verification within a period of 5-years or when the Company enters into a service agreement with the customer for provision of the specific services.

Services that require the application of CDD in relation to business relationship include:

- virtual currency services;
- issue of negotiable instruments;
- foreign exchange;
- transmission of funds by or through any means.

Keeping customer information up to date

The Company takes steps from time to time to ensure that the customer information that has been obtained is up-to-date and relevant. To achieve this, Company undertakes periodic reviews of existing records of customers.

An appropriate time to do so is upon certain trigger events such as:

- specific time period has passed and the customer's risk profile shall be reviewed;
- the customer notifies about changes in the customer´s identification information, such as name, address, occupation or nature of business, etc.;
- when a significant transaction (not only of a big amount, but also suspicious) is to take place;
- when a material change occurs in the way the customer's account is operated;
- when the customer's documentation standards change substantially;
- when the Company is aware that it lacks sufficient information about the customer concerned.

In addition to aforementioned, the customers are continuously (when any of watchlists is updated) screened against watchlists (incl. PEP, Sanctions and Adverse Media). In case of match – the Company is notified and shall apply CDD accordingly.

Exceptions to CDD application requirements

When the Company has previously identified and verified a person or an entity using methods specified above and keeping all the records with associated information, the Company does not have to apply CDD measures for re-identification unless there are doubts about the accuracy of information used. The Company may be required to simply review and update the customer's information (e.g., name, address, etc.) in line with best practice and risk assessment procedure.

In addition, the Company does not have to apply CDD measures in the following cases

- when the customer who conducts cash transactions that exceed $10,000 is a financial entity/public body or the amount is deposited to a business account/automated banking machine;
- when the customer who conducts virtual currency transactions that exceed $10,000 is a financial entity/public body;
- when the Company transfers or receives virtual currency as compensation for the validation of a transaction that is recorded in a distributed ledger;
- when the Company exchanges, transfers or receives nominal virtual currency amount for the validation of transaction or transfer of information;
- when the customer conducts or attempts to conduct suspicious transaction, however the Company has already verified the identity, has no doubts about the accuracy of information or believes that the new application of CDD make the customer informed about the reporting procedure;
- when there is a transaction between an employer and employee under service agreement
- when the information record is created about the public body, corporation or trust with $75 million net assets and their subsidiaries.

Know Your Customer: on-boarding principles

The Company has established customer's onboarding procedure as separate document (annex 4), which contains the steps, which should be performed for application of CDD measures in the course of customer's onboarding, as well as certain requirements for documents and data to be provided. The customer's onboarding procedure established follows the abovementioned requirements.

Identification of the customer – natural person

In the course of customer's onboarding procedure, the Company shall identify the customer and verify the identity of the customer who is a natural person and, where relevant, their representative by using any of the methods specified below and referring to these documents, data or information provided by a reliable and independent source that is required for each specific method.

Methods of verification for a natural person include:

- government-issued photo identification method (incl., remote);
- credit file method;
- dual-process method;
- affiliate or member method;
- reliance method.

Government-issued photo identification method

If the Company applies government-issued photo identification method, the following data shall be collected and retained for the identification and verification of the customer:

- person's name;
- photograph;

- date of verification;
- type of document;
- unique identifying number of the document used;
- place of issue and expiry date (if available).

The following documents which contain data specified for the government-issued photo identification method may be used as the basis for the identification of a natural person:

- an identity document or citizenship card issued by the government of Canada;
- an identity document issued by a foreign government if it is equivalent to a Canadian document;
- Canadian permanent resident card;
- Canadian provincial or territorial driver's license.

In addition, the aforementioned documents must meet all the requirements in order to use them for the identification of a natural person. The document must:

- be authentic, current and valid;
- be issued by a federal, provincial or territorial government (or by a foreign government if it is equivalent to a Canadian document) ;
- indicate the person's name;
- include a photo of the person;
- include a unique identifying number; and
- match the name and appearance of the person being identified.

The document is considered acceptable if it has been issued by Canadian or foreign municipal governments. The authenticity and validity of the document can be examined in person or in presence of the person being identified. The Company must be able to review the original physical document and its security features with the aim of ensuring that the document meets the requirements specified previously.

Remote government-issued photo identification method

In case the customer and where relevant, their representative is identified without their physical presence via remote onboarding, the customer and the representative still can be identified via the government-issued photo identification method in accordance with the requirements by establishing additional remote authentication procedure that allows the Company to examine the identification document. The procedure implies the use of technological means of authentication to ensure the fulfillment of requirements.

The procedure includes the following steps to assess the authenticity of the document:

- the Company shall request a scan of the identification document from the customer;
- the Company shall use a technology to compare the features of the identification document against its' characteristics (e.g., size, texture, spacing, lettering, etc.), security features (e.g., watermarks, electronic chips, etc.) or markers (for example, logos, symbols).

In order to determine if the provided document is valid and current, the procedure includes the following measures:

- the Company shall participate in direct video streaming for the onboarding if the facial image of the customer and the original of the identification document shown by the customer is recorded at the time of direct video streaming; or
- the customer shall use virtual application means by taking a “selfie“ using the camera on any proper electronic device and application to apply facial recognition technology to compare the features of that "selfie" to the photo on the authentic government-issued photo identification document[9].

Such technological means for the customer’s onboarding can be used only if all the following requirements are fulfilled:

- the Company has established and approved by the Senior Management and the Compliance Officer list of technological means, which may be used by the Company for the customer’s onboarding;
- the Company has established the customer’s onboarding procedure which allows to use certain technological means for the customer’s onboarding;

[9] The Company must apply only one of the measures provided.

- the Company has established adequate internal control measures to ensure fulfillment of aforementioned requirements.

The customer is identificated and the customer's identity is verificated using such remote alternative method if the Company successfully determines that the government-issued photo identification document is authentic, valid, current and ensures that the name and photo match the name and appearance of the customer.

Credit file method

If the Company applies credit file method, the following data shall be collected and retained for the identification and verification of the customer:

- person's name;
- address;
- date of birth;
- credit file number;
- date of credit file search and name of the credit bureau or third-party vendor.

The Company shall derive data specified for the credit file method from the customer's credit file and request information directly form the customer in order to compare the name, address and date of birth. The credit file information for the identification purposes can be provided only by Equifax Canada, TransUnion Canada or authorized third party vendor and searched at the time of verification process.

The credit file as the main document for identification under credit file method must meet certain requirements. The credit file must:

- contain valid and current information;
- be obtained from a Canadian credit bureau (not foreign credit bureaus) ;
- be in existence for at least 3 years;
- contain information that is derived from more than one source;
- match the name, address and date of birth of the person being identified.

In addition, the Company shall consider the following circumstances while matching the information obtained from the customer with the information from credit file:

- typo in the address or name;
- discrepancy in date of birth;
- multiple addresses.

Typo in the address is not critical to the identification of the customer and depends on the decision of the Company. Discrepancy in date of birth does not allow the Company to rely on such information, so the Company shall use another credit file or method of identification. Provision and determination of multiple addresses is acceptable if the credit file indicates the provided address as secondary.

Dual-process method

Dual-process method stands for the use of **two** categories of information and sources in a single onboarding process. In course of dual-process method identification, the Company shall consider performing the following actions and obtaining the following categories of data:

- referring to information that includes the customer's name and address and confirming that information;
- referring to information that includes the customer's name and date of birth, and confirming that information;
- referring to information that includes the customer's name and confirms that they have a deposit account, a prepaid payment product account, or a credit card or other loan account with a financial entity and confirming that information.

Using two categories of data information means that the Company combines and verifies, for example, the name and address with the name and date of birth, the name and address with a financial account or the name and date of birth with a financial account of the customer. The Company shall ensure that the information matches with the information provided by the customer.

There are different reliable sources of information for each category of information that shall be used for dual-process method, and which are specified in a separate document **(annex 5).** The Company must not use the same source for the two categories of information. The information that the Company referrers to must be valid and current.

Affiliate or member method

If the Company applies affiliate or member method, the following data shall be collected and retained for the identification and verification of the customer:

- person's name;
- address;
- date of birth;
- records of the affiliate or member.

The information from the following entities is required in order to verify the customer's identity

- affiliate of the Company that performs activities specified in paragraph 5(a) to (g) of the PCMLTFA;
- foreign affiliate if the Company that performs similar activities as referred above outside of Canada;
- financial entity that is a member of the same financial services cooperative or credit union central.

The Company shall compare and match the information provided by the affiliate or member with the information provided by the customer. In order to use this method, the affiliate or member must have previously verified the customer's identity by using any methods mentioned in this Program or methods that were applicable prior to June 1, 2021. If there are doubts about the accuracy of information or application of methods, the Company shall re-verify the identity of the customer.

Identification of the customer – legal entity

The Company identifies the customer and verifies the identity of the customer who is a legal entity and their representative by using any of the methods specified below and referring to these documents, data or information provided by a reliable and independent source that is required for each specific method. The methods for identification of a legal entity include:

- confirmation of existence method;

- reliance method.

Confirmation of existence method

If the Company applies affiliate or member method, the following data shall be collected and retained for the identification and verification of the customer:

- business name;
- business address;
- registration number (if any).

The following documents which contain data specified for the confirmation of existence method may be used as the basis for the identification of a natural person:

- partnership agreement;
- articles of association;
- the most recent version of any other record that confirms its existence and contains its name and address;
- record from a publicly accessible database.

The records that the Company is referring to must me authentic, valid and current.

Reliance method

The Company can obtain information about the customer who is a natural person or an entity (applicable for both) from another person or entity referred to in section 5 of the PCMLTFA, or affiliated foreign entity that performs similar activities outside of Canada referred to in section 5(a) to (g) of the PCMLTFA.

The affiliated foreign entities shall meet the following requirements:

- they have established policies related to the record keeping, verifying identity, and compliance program requirements, including the requirement to develop risk assessment policy and take enhanced measures where the risk has been identified as high;
- their compliance with aforementioned policies is subject to the supervision of a competent authority under the legislation of that foreign state.

This reliance method of the customer's onboarding can be used only if all the following requirements are fulfilled:

- the Company has obtained the information from the other RE or affiliated foreign entity that was used to confirm the identity of the customer;
- the Company got satisfied that the information is valid, current and the customer's identity was verified by referring to a record as described in the confirmation of existence method above, or if any other applicable measures were performed prior to June 1, 2021;
- the Company has a written agreement or arrangement with the other RE or affiliated foreign entity that requires them to provide the Company with all of the information about the customer .

The Company verifies the correctness of the customer's data specified above, using information originating from a publicly accessible database or credible and independent source for that purpose. Where the Company has access to the relevant register of legal entities, the submission of the documents specified above do not need to be demanded from the customer.

The identity of legal entity and the right of legal entity's representation can be verified on the basis of a document specified above, which has been authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions, thereby using at least two different sources for verification of data in such an event.

The identification of the customer's representative and their right of representation

The representative of the customer who intends to act on the customer behalf shall be identified as the customer, who is a natural person in accordance with aforementioned onboarding requirements. The Company must also identify and verify the nature and scope of the right of representation of this representative. The name, date of issue and name of issuer of the document that serves as a basis for the right of

representation must be ascertained and retained, except in case, when the right of representation was verified using information originating from the relevant register and information about such verification is saved.

In case when the customer is a legal entity, the following persons may be deemed as the customer's representative:

- the natural person, whom right to represent the customer arises from law (e. g. management board member, director, manager, or similar position; hereinafter – lawful representative);
- the natural person to whom the relevant power of attorney is issued by the person specified in previous point (hereinafter – contractual representative).

The Company must observe the conditions of the right of representation granted to the legal entity's representatives and provide services only within the scope of the right of representation.

The authorisation has to be in line with the requirements of the Canadian laws and regulations. The authorisation issued abroad has to be legalized for use in Canada in case the right of representation of the customer (legal person) is evident from the registry extract, articles of association or equivalent documents evidencing the identity of the customer (legal person), a separate document of authorisation (e.g., a power of attorney) should not be required.

The identification of the customer's Beneficial Owner

The beneficial owner means any natural person who owns the customer (a legal person or a foreign undertaking) or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted.

The Company has established beneficial owner identification guidelines as separate document (annex 6), in accordance which the Company identifies the beneficial owner of the customer and takes measures to verify the identity of the beneficial owner to the extent that allows the Company to make sure that they know who the beneficial owner is. The Company collects the following data regarding the customer's beneficial owner(s):

- name(s) and surname(s);
- address(es)

- information about the ownership, control and structure of the entity

The Company shall request from the customer information about the customer's beneficial owner and supporting official documentation (e. g. providing the customer with an opportunity to specify their beneficial owner when collecting data about the customer), conduct an open-source search or consult publicly available information.

The Company shall take reasonable measures to confirm the accuracy of the beneficial ownership information (incl. data about being a member of a group and the ownership and management structure of the group), which may include referring to official documentation or records (e.g., minute book, shareholders register, articles of incorporation, etc.).

If the Company is unable to obtain the beneficial ownership information, it is necessary to take reasonable measures to verify the identity of the entity's chief executive officer or of the person who performs that function and apply the special measures for high-risk clients for better understanding and establishment of the overall ownership, control, and structure picture.

Identification of the purpose and nature of the business relationship or a transaction

The Company shall understand the purpose and nature of the establishing Business Relationship or performing transaction. Depending on the Company risk assessment of the situation, measures required may include:

- the customer confirming that the Company's terms of services provision are accepted;
- the customer providing additional information in regards of transaction(s) performed (e. g. in the course of EDD measures or monitoring of the business relationship as specified below).

The Company shall apply additional measures and collect additional information to identify the purpose and nature of the Business Relationship or an Occasional Transaction in cases where:

- there is a situation that refers to high value or is unusual;

- where the risk and/or risk profile associated with the customer and the nature of the business relationship gives reason for the performance of additional actions in order to be able to appropriately monitor to business relationship later (e. g. if the customer is residing or established in high-risk third countries).

Politically Exposed Person's or Head of International Organization's identification

Politically exposed person (PEP) means the natural persons who are or have been entrusted with prominent public functions. PEPs include close family members or close associates of such persons.

Prominent Public Functions means:

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

Head of international organization (HIO) means the natural persons who hold or has held specific office or position of head of an international organization. HIOs include close family members or close associates of such persons.

International organization means:

- international organization established by the governments of states;
- institution of an organization referred above;

- international sports organization.

Close Family Member means the spouse or common-law partner, biological or adoptive child(ren), mother(s) and father(s) and their spouse or partner, brother(s) and sister(s) of a PEP/HIO.

Close Associate is a natural person who:

- is a business partner of, or who beneficially owns or controls a business with, a PEP/HIO;
- is in a relationship with PEP/HIO;
- is involved in financial transactions with a PEP/HIO;
- serves as a member of the same political party or board as a PEP/HIO;
- carries out charitable works with a PEP/HIO;
- is listed as joint on a policy where one of the holders might be a PEP/HIO.

The Company takes measures to ascertain whether the customer, the beneficial owner of the customer or the representative of the customer is a PEP, their family member or close associate or if the customer has become such a person. For that purpose the Company:

- asks the customer about their status in the course of the customer's onboarding;
- makes reference to publicly available information;
- screens relevant persons against commercially available databases for determining whether a customer or a beneficial owner of a customer is a PEP.

Where the customer who is a PEP no longer performs important public functions placed upon them, the Company shall at least within 5 years take into account the risks that remain related to the customer and apply relevant and risk-based measures as long as it is certain that the risks characteristic of PEPs no longer exists in the case of the customer.

Enhanced due diligence measures

The Company applies Enhanced Due Diligence (EDD) measures where the customer and product/service combination is considered to be a greater risk. This higher level of due diligence is required to mitigate the increased risk. A high-risk situation generally occurs where there is an increased opportunity from money laundering or terrorist financing through the service and product the Company provides or from a customer of the Company.

What the EDD actually entails will be dependent on the nature and severity of the ML/TF risk.

High-risk situations

In any situation that by its nature presents a higher risk of ML/TF, Company takes additional measures to mitigate the risk of ML/TF. The Company applies EDD measures, when:

- the customer's risk profile indicates high risk level of ML / TF;
- upon identification of the customer or verification of submitted information, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner (incl., complex structure that conceals the identity of beneficial owners);
- where the customer is a financial institution with which the Company has a correspondent banking relationship, or the customer is a correspondent bank that has been subject to sanctions;
- in the case of performance of transaction or business relationship with the PEP/HIO, the family member of the PEP/HIO or a person known to be the close associate of the PEP/HIO;
- where funds transfers and transfers of high value from personal or business accounts are frequently conducted to or from high-risk jurisdictions and financial secrecy jurisdictions;
- the customer has connection with such country or territory or is from such country or territory or their place of residence or seat or the seat of the payment service provider of the payee is in a country or territory that, according to credible sources such as mutual evaluations, reports

or published follow-up reports, has not established effective AML/CTF systems that are in accordance with the recommendations of the FATF or FINTRAC.

Prior to applying EDD measures, the Company ensures that the business relationship or transaction has a high risk and that a high-risk rate can be attributed to such business relationship or transaction. Above all, the Company assesses prior to applying the EDD measures whether the features described above are present and applies them as independent grounds (that is, each of the factors identified allows application of EDD measures with respect to the customer).

Scope of EDD measures

In case when EDD measures must be applied, the amount of EDD measures and the scope shall be determined by the Company's employee, who is applying such measures. The following additional and relevant due diligence measures may be followed:

- obtaining additional information about the customer (e.g., occupation, volume of assets, information available through public databases, Internet, etc.);
- obtaining additional information about the intended nature of the business relationship, SoF and SoW of the customer ;
- obtaining information about the reasons for intended or conducted transactions;
- obtaining additional documents, data, or information; or taking additional steps to verify the documents obtained;
- increased monitoring of transactions of higher/risk products/services/channels;
- establishing transaction thresholds;
- increasing internal controls of high-risk business relationships;
- obtaining the approval of senior management at the transaction level for products and services that are new for the customer.

The Company establishes procedure for application of EDD measures as separate document (annex 7), which specifies criteria for application of certain EDD measures, as well as procedure for such measures' application.

High-Risk third countries

With respect to business relationships or transactions involving natural persons residing or legal persons established in high-risk third countries[10] as identified by FATF, the Company applies the following EDD measures:

- obtaining additional information on the customer and on the beneficial owner;
- obtaining additional information on the intended nature of the business relationship;
- obtaining information on the source of funds and source of wealth of the customer and of the beneficial owner;
- obtaining information on the reasons for the intended or performed transactions;
- obtaining the approval of Compliance Officer for establishing business relationships with these customers or continuing business relationships with them;
- conducting enhanced monitoring of the business relationship with these by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
- ensuring that the first payment be carried out through an account in the customer's name with a credit institution, where the credit institution is registered in Canada or in a third country which imposes requirements equivalent to those laid down by Law and is supervised by competent authorities for compliance with those requirements.

When applying EDD in the cases where transactions and business relationships are carried out with natural persons residing or legal persons established in high-risk third countries (identified according to lists of jurisdictions with strategic deficiencies in their frameworks to combat ML and/or TF published by the FATF on ML and TF), and in the cases where higher risk of ML and/or TF is identified based on the risk assessment made by the Company, the Company shall apply one or several additional measures to identify the customer and of the beneficial owner to decrease the risks posed and must:

- obtain approval from the Compliance Officer for establishing business relationships with such customers or continuing business relationships with these customers;
- take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;

[10] https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-june-2023.html

- perform enhanced ongoing monitoring of the business relationships with such customers.

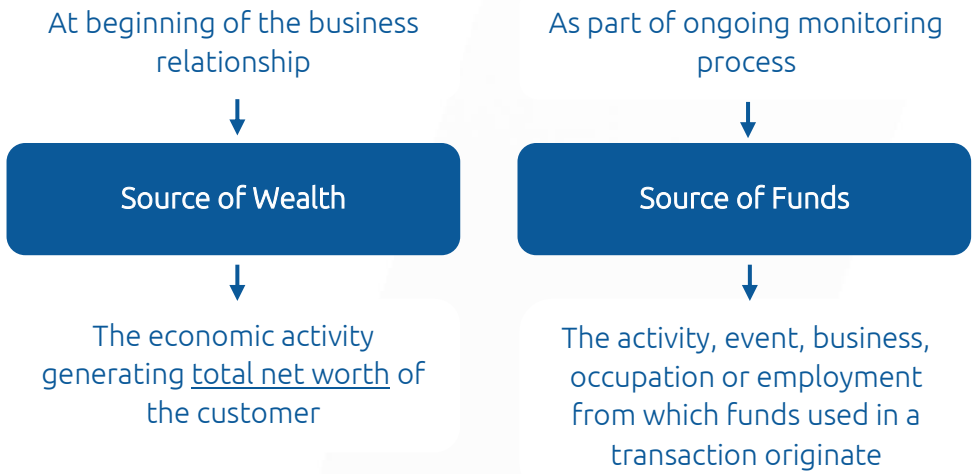
Source of Wealth and Funds

Establishing the customer's source of wealth (SoW) and source of funds (SoF) is a core requirement of EDD.

Source of Wealth refers to the origin of the customer's entire body of wealth (i.e. total assets). SoW explains activities the customer participates in and their geographical location. This information will usually give an indication as to the volume of wealth the customer could be expected to have, and a picture of how the customer acquired such wealth. When establishing SoW, there is no need to establish funds used in specific transaction. The goal of SoW establishment is to understand and verify, that customer´s SoW corresponds with data given by the customer when onboarding and volume of the customer´s wealth allows them to perform transactions with expected turnover specified by the customer.

Source of Funds refers to origin of funds being deposited, received, or transferred with the Company. SoF tells where the assets is coming from, which can be proven through bank statements, tax returns or the customer´s financials, etc. Typically, SoW is requested when establishing business relationship or performing EDD, SoF is requested when there is a need to understand what the origin of a transaction is.

The types of data and documents that can be used for verification will vary depending on the circumstances and the information that the customer provides to the Company. The Company collects information relating to SoW or SoF of its customers and, according to the level of risk involved, takes reasonable steps to verify that information.



The types of data and documents that can be used for verification will vary depending on the circumstances and the information that the customer provides to Company.

The following documents, data, or information could be considered reliable and independent:

- government-issued or registered documents or data;
- full bank and other investment statements;
- full payslips or wage slip or other documents confirming salary;
- inheritance (stamped grant of probate, stamped grant of letters of administration);
- audited financial accounts from a chartered accountant or Charities Services;

- letter from an agent of the customer confirming they have knowledge of and established business relationships with the customer;
- a copy of a will;
- sales and purchase agreements.

For customers who conduct their business with Company there is a range of documents that Company can use to verify how funds have been acquired (e.g., balance statements and other accounting documents, contract with counterparties, invoices, proof(s) of work, etc.).

The company establishes limits on the volume of transactions, after which the source of funds must be requested, in the requirements for transactions monitoring (as specified below).

Ongoing monitoring

In the course of the **ongoing monitoring of the business relationship**, the Company monitors the transactions concluded during the business relationship in such a manner that the Company can determine whether the transactions to be concluded correspond to the information previously known about the customer (i.e., what the customer declared upon the establishment of the business relationship or what has become known in the course of the business relationship).

The Company also monitors the business relationship to ascertain the customer's activities or facts that indicate criminal activities, ML/TF or the relation of which to ML/TF is probable, incl. complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or that are uncharacteristic of the specific features of the business in question. In the course of the business relationship, the Company constantly assesses the changes in the customer's activities and assesses whether these changes may increase the risk level associated with the customer and the business relationship, giving rise to the need to change the customer's risk level assigned and to apply EDD measures.

The Company establishes and maintains the **requirements for transactions monitoring** as separate document (annex 8), which contains set of measures shall be applied in the course of ongoing monitoring of the business relationship.

Risk-based approach to monitoring

The extent of ongoing monitoring is linked to the determined customer's risk profile. The Company takes additional measures when monitoring the business relationships posing a higher risk. High-risk customers, for example PEPs, require more frequent and intensive monitoring.

The Company conducts ongoing monitoring on a risk-based approach and considers:

- the nature and type of transactions (e.g., abnormal size or frequency);
- the nature of a series of transactions (e.g., a number of transfers);
- the amount of any transactions, paying particular attention to particularly substantial transactions;
- the geographical origin/destination of a deposit or withdrawal;

- the customer's normal activity or turnover;
- specific transactions patterns, published by relevant authorities (e. g. FINTRAC or FATF);
- results provided by VC wallets scoring solutions used.

The Company is vigilant for changes on the basis of the business relationship with the customer over time, which may include:

- new products or services that pose higher risk are entered into;
- new corporate or trust structures are created;
- the stated activity or turnover of the customer changes or increases;
- the nature of transactions changes or their volume or size increases etc.

Where the nature of the business relationship changes significantly, the Company carries out applies relevant measures to ensure that the ML/TF risk involved, and nature of the business relationship are fully understood by the Company. Ongoing monitoring procedures take account the above changes.

Methods and procedures

When considering how to monitor its business relationship with the customer, the Company takes into account the following factors:

- the size and complexity of the Company's business;
- its assessment of the ML/TF risks arising from the Company's business;
- the nature of the Company's systems and controls;
- the monitoring procedures that already exist to satisfy other business needs of the Company;
- the nature of the products and services (which includes the means of delivery or communication).

The Company takes the four steps systemic approach for ongoing monitoring of the business relationship:

Measures, used by the Company for ongoing monitoring of established business relationships is divided into two following categories.

Screening – monitoring transactions in real-time in real time on the basis of the parameters or characteristics previously determined. Screening measures are applied to the transaction before or immediately after completion of the transaction and may require the following actions:

- transaction suspension or rejection;
- application of EDD measures (incl. identification of SoF and the purpose of transaction);
- re-assessment of the customer's risk profile;
- sending an internal report to the Compliance Officer;
- sending an external report to the FINTRAC.

Monitoring – analysis of transactions after their performance for the purpose to identify transactions and circumstances that could not be identified in real time or that, due to the nature of the transaction, did not appear in the parameters of screening. Monitoring measures may require the following actions:

- account suspension;
- application of EDD measures (incl. identification of SoF and the purpose of transaction);
- re-assessment of the customer's risk profile;
- sending an internal report to the Compliance Officer;
- sending an external report to the FINTRAC.

In both cases (screening & monitoring), the Company uses technological solutions (incl. third-party solutions), as well as appoints employees responsible for the ongoing monitoring of the business relationships in according with requirements established.

Suspicious Transactions Indicators

When establishing and maintaining requirements for ongoing monitoring of the business relationship, the Company takes into account the Guidance issued by FINTRAC, as well as other sources, incl. guidelines of international organizations (e. g. FATF). The following are some of the suspicious activity indicators most commonly associated with ML:

- large or frequent deposits or withdrawals;
- suspicious activity based on transaction pattern, i.e.
  - account used as a temporary repository for funds;
  - a period of significantly increased activity amid relatively dormant periods;
  - "structuring" or "smurfing" i.e. many lower value transactions conducted when one, or a few, large transactions could be used;"
  - U-turn" transactions, i.e. funds pass from one person to another, and then back to the original person or company;
  - excessive transactions just below established thresholds (e. g. reporting, CDD/EDD limits, etc.);
  - excessive transfers between several counterparties.
- involvement of one or more of the following entities which are commonly involved in ML:

    - shelf or shell company;
    - company registered in a known "tax haven" or “off-shore” financial center;
    - company formation agent, or secretarial company, as the authorized signatory of the bank account;
    - money service operator;
    - casino;
- the customer refuses or is unwilling to provide documents or information necessary to determine the customer’s or the beneficial owner’s identity or submits documents or information that raise doubts about their veracity, authenticity, etc.;
- the customer refuses or is unwilling to provide information or documents necessary for the business relationship monitoring (e.g. explanation of their activity, information about their SoW/SoF) or submits documents or information that raise doubts about their veracity, authenticity, etc.;
- activity is incommensurate with that expected from the customer considering the information already known about the customer (e.g. SoW, country of residence or establishment) and the customer’s previous activity;
- deposits from or withdrawals to a virtual currency address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports;
- currencies, countries or residents of countries, commonly associated with international crime, drug trafficking, terrorist activities or the persons or organizations designated as terrorists or their associates, or identified as having serious deficiencies in their anti-money laundering regimes;
- PEPs and close family members or close associates of such persons.

The detection of such indicators is subject to reporting obligation of the Company, that must be used as the basis for submitting specific reports. The occurrence of one indicator in relation to transaction does not mean that it is suspicious and should be immediately reported as it should be supported by relevant facts and context.

The extended list of other ML/TF indicators of suspicious activities and transactions (incl., virtual currency indicators, TF risk indicators) is provided in a separate document (annex 9). The indicators include potential red flags for suspicious characteristics, behaviors, patters and other factors that determine irregularities related to suspicious transactions, which were developed by FINRAC based on reviews of multiple ML/TF cases and FATF publications.

Sanctions policies

In addition to AML/CTF framework, this Program also covers the Company's obligations related to implementation of sanctions legally binding to the Company. The Company follows the Guidance, issued by FINTRAC and FATF and takes measures to ensure compliance with the relevant regulations and legislation on sanctions in Canada. It is particularly vital that the Company is able to identify sanction subjects and transactions violating sanctions, which may arise in the course of the Company's business activity. The Company takes into account at least the following sanction regimes:

- Canadian Economic Sanctions;
- Freezing Assets of Corrupt Foreign Officials Act sanctions;
- UN Sanctions;
- Canadian Autonomous Sanctions.

By the decision of the Compliance Officer, the Company may follow other sanction regimes and restrictive measures.

Procedure for identifying the subject of sanctions and a transaction violating sanctions

The Company verifies whether the customer or their beneficial owner is a subject of Sanctions in the course of the customer's onboarding procedure.

To avoid establishing business relationship or conducting transactions with any subjects of sanctions, the Company implements an effective screening mechanism, which includes:

- screening customers and beneficial owners of customers against sanctions watchlists at the establishment of the Business Relationship;
- screening the customers and the Beneficial Owners of the customers against sanctions watchlists as soon as practicable (i. e. when any of watchlists has been updated);
- screening of transactions (incl. scoring of VC wallets) for the purpose to identify connection to subjects of sanctions.

To verify that the persons' names resulting from the inquiry are the same as the persons listed in the document imposing sanction(s), their personal data shall be used, the main characteristics of which are, for a legal entity, its name or trademark, registry code or registration date, and for a natural person, their name and date of birth. In order to establish the identity of the persons specified in the relevant legal act or notice being the same as those identified as a result of the inquiry from databases, the Company analyzes the names of the persons found as a result of the inquiry based on the possible effect of factors distorting personal data (e. g. transcribing foreign names, different order of words, substitution of diacritics or double letters etc.).

If sanctions subject is identified – the relevant notice must be sent to the Compliance Officer. If the Company's employee has doubts that a person is a subject of sanctions, this employee shall immediately notify the Compliance Officer. In this case the Compliance Officer shall decide on whether to ask or acquire additional data from the person or notify the FINTRAC immediately of their suspicion.

Actions when identifying the sanctions subject or a transaction violating sanctions

If the Company becomes aware that the customer which is in the business relationship with the Company, as well as a potential customer intending to establish the business relationship or to perform a transaction with the Company, is the subject of sanctions, the Company's employee shall immediately notify the Compliance Officer about the identification of the subject of sanctions, or the doubt thereof.

The Company will not establish business relationship with potential customers subject to Sanctions.

Depending on sanction regime imposed, if the subject of sanctions or transaction violating sanctions are identified, the following actions must be taken:

- the Company shall refuse to perform transaction or establish the business relationship;
- the Company shall terminate the business relationship and freeze the customer's assets;
- the Compliance Officer must inform the FINTRAC about sanction implemented;
- the Company shall wait for further instructions from the FINTRAC regarding actions shall be taken.

When identifying the subject of the sanctions, it is necessary to identify the measures that are taken to sanction this person. These measures are described in the legal act implementing sanctions, therefore it is necessary to identify the exact sanction what is implemented against the person to ensure legal and proper application of measures.

Reporting

Internal reporting

There is a statutory and regulatory obligation on the Company to disclose information to the Compliance Officer in circumstances where they:

- know or suspect, or
- have reasonable grounds for knowing or suspecting, that another person is engaged in money laundering or terrorist financing.

The Company's employees must disclose not only when they have actual knowledge or suspicion of ML or TF but also if, in the circumstances, they should have reached that conclusion and failed to do so. Any knowledge or suspicion must be reported to the Compliance Officer as soon as possible as provided below. Employees must not delay any disclosures unnecessarily.

In case when necessity to notify the Compliance Officer arise, such notification shall be performed by filling **internal report in the form** approved **(annex 10)**. Internal report shall be prepared and signed by the employee. Signed internal report shall be sent to the Compliance Officer's email as soon as possible but not later than 24 hours after necessity to send report has arisen.

It should be note that if the necessity of internal report arises, the Company must immediately postpone the transaction (if possible).

The Compliance Officer shall immediately analyze the report received and take necessary actions (e. g. sending external report, terminate the transaction or the business relationship, perform further investigation, etc.).

External suspicious transaction reports (STR)

The Company must suspend the transaction disregarding the amount of the transaction (except for the cases where this is objectively impossible due to the nature of the transaction, the manner of execution thereof or other circumstances) and the Compliance Officer must report to the FINTRAC on the activity or the circumstances that they identify in the course of economic activities and whereby:

- the Company has established that the customer is carrying out a suspicious transaction;
- the Company has reasonable grounds to suspect that a transaction that occurs or is attempted in the course of the customer's activities is related to the commission or the attempted commission of an ML/TF offence.

Suspicious monetary operations or transactions shall be determined by taking the following measures:

- screening and identifying suspicious transactions;
- assessing the facts and context relating to the suspicious transaction;
- applying ML/TF indicators to the assessment of the facts and context;
- explanation of the grounds for suspicion in an STR form.

The report specified above must be made before the completion of the transaction if the Company suspects or knows that ML or TF or related crimes are being committed and if said circumstances are identified before the completion of the transaction.

The Compliance Officer is responsible to submit the external reports to FINTRAC. The Compliance Officer keeps a track of all internal investigations and escalations performed in the format, which may be reproduced in writing.

When suspicious monetary operation or transaction is detected, a documented investigation must be completed, that operation or transaction must be suspended, and a report made to the FINTRAC as soon as practicable after suspicious activity determination, application of measures and achievement of established threshold. There is no specific monetary threshold, whereas the STR might contain transactions that are subject to other types of reports. STR may include one or up to 99 transactions that have the same status and originate form same location (more than 99 require a separate STR).

Suspicious transaction report to the FINTRAC shall be made in accordance with guidelines on Suspicious Transaction Report[11], Validation Rules and Forms approved by FINTRAC **(annex 11)**.

Reasonable grounds to suspect

Reasonable grounds to suspect (RGS) means a likehood that a transaction might be related to an ML/TF offence, which is pursued as a higher threshold requirement for submitting an STR to FINTRAC. This is a strong suspicion without any prejudices that can be reached through the consideration and review of the following elements:

- verified facts of probability that an ML/TF offence has occurred (incl., date, time, location, amount or type of transaction);
- context of transaction (i.e., information that explains all the circumstances or transaction);
- ML/TF indicators related to a transaction (**annex 9**).

The threshold is reached if the Company is able to present a range of provable and supportive facts towards the suspicion of ML/TF offence. The reasonable grounds for suspicion do not have to be proven or otherwise verified.

24-hour rule

The 24-hour rule is a requirement to unite several transactions in a single transaction that total $10,000 or more, which shall be conducted by the same person, on behalf of that person, or for the same beneficiary within a period of 24-hours. The rule is subject to the CDD and subsequent reporting requirements for large cash or virtual currency transaction(s) and electronic funds transfer if they exceed the established threshold.

Transactions that fall under the 24-hour rule include:

- one transaction exceeding $10,000;

[11] https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/Guide2/2-eng

- several transactions under $10,000 that exceed the threshold being aggregated;
- one or several aggregated transactions of $10,000.

Tipping off

It is a criminal offence for anyone, following a disclosure to a nominated officer or to the appropriate institution, to do or say anything that might either "tip off" another person that a disclosure has been made or prejudice an investigation. When the customer is the subject of an external reporting, there must be taken careful steps while communicating with the customer and additional advice should be taken from the Compliance Officer in order not to accidentally disclose investigative actions to the customer.

The Company's employees are prohibited to inform a person, its beneficial owner, representative or third party about a report submitted on them to the FINTRAC, a plan to submit such a report or the occurrence of reporting as well as about a precept made by the FINTRAC or about the commencement of criminal proceedings.

Submission and validation of report

After the Company submits the STR report in accordance with all requirements, FINTRAC reviews the report to ensure the provision and accuracy of mandatory information. Therefore, the submitted report goes through the validation process under specific validation rules (annex 12) established by FINTRAC. The purpose of validation rules is to identify possible problems and gaps in provided information. The rules are different depending on the type of validation process that include:

- web report validation;
- batch report validation.

Web reporting (F2R) is a process that enables an immediate electronic validation of STR. In case the system detects any incorrect or improperly formatted information, the Company must correct all indicated errors for mandatory field and submit an STR. To gain access to FINTRAC web reporting, the Company shall send an email to F2R@fintrac-canafe.gc.ca and provide all necessary information (incl., business name, address, type of report, name of reporting administrator).

Batch reporting is the submission of multiple reports (up to 10,000) in one batch file that shall be formatted in accordance with FINTRAC's specifications for the purpose of validating the file against the violation of validation rules. In case the file contains errors of structure or format, FINTRAC rejects the file, and the Company must resubmit the documents correctly. In case of potential issues, the file will be accepted but the Company shall review the submitted information. In order to use batch reporting system for verification and reporting, the instruction shall be considered for the following:

- installation of batch transmission software provided by FINTRAC;
- enrollment into F2R;
- application for a public key infrastructure (PKI) certificate.

The STR mentioned in this chapter shall be sent through a web reporting system or batch file transfer as explained above in accordance with Suspicious Transaction Report Specifications, Standard Batch Reporting Instructions and Specifications, Validation Rules and Forms approved by FINTRAC **(annex 11)**.

External terrorist property reports (TPR)

The Company must immediately disclose the existence of property in their possession or control that they know is owned or controlled by or on behalf of a terrorist group or listed person, as well as the information about any transaction in relation to that property to the RCMP or to the CSIS. Such property for the purpose of a TPR include cash, monetary instruments, virtual currency, accounts, prepaid payment products and their accounts, securities, jewellery, precious metals or stones, real estate, insurance policies and casino products. The company is prohibited to conduct or complete any transactions in relation to the mentioned properties.

Terrorist group is an entity or association (incl., listed) that facilitates or carries out terrorist activities, which can be determined through:

- publicly available information or media;
- publicly available lists of terrorist activities (e.g., the Office of Foreign Assets Control (OFAC) and European Union (EU) lists).

Listed person is a person or an entity who is listed in the Schedule of the RIUNRST and who gives reasonable ground to suspect that this person/entity:

- has carried out or facilitated a terrorist activity;
- is controlled by such person/entity;
- is acting on behalf of such person/entity.

The TPR shall be submitted after disclosure of information to RCMP or CSIS in accordance with specified lists and sent to FINTRAC in accordance with the requirements of reasonable grounds to suspect and approved Forms (annex 11) by fax or mail. In order to submit TPR to FINTRAC, a specified transaction or attempt as a ground for TPR might not be yet conducted. The threshold for submitting TPR is same as for STR.

External amount-based transaction reports (LCTR/LVCTR)

The Company through the Compliance Officer must send information on the customer's identity data and information on performed cash or virtual currency transactions to the FINTRAC not later than within 15 calendar days after the identification of cash transactions or within 5 working days in case of transactions in virtual currency, if the daily value of such transaction(s) is equal to or exceeds $10,000 or the equivalent amount in foreign or virtual currency, regardless of whether the transaction is concluded in one or more related transactions within 24 hours period. The value of the virtual currency is determined at the time of the transaction performed.

In case of cash transactions information submitted to the FINTRAC for LCTR shall include:

- the data confirming the customer's identity, and where the transaction is carried out through a representative – also the data confirming the identity of the representative;
- the amount of the transaction;
- the currency in which the transaction was executed;
- the date of execution of the transaction;
- the manner of execution of the Monetary Operation;
- the entity for whose benefit the Monetary Operation was executed (if it's possible);

- other data specified in the relevant FINTRAC instructions.

In case of virtual currency transactions information submitted to the FINTRAC for LVCTR shall include:

- the information about the Company, the reporting entity, and 24-hour period;
- the data about any transactions being reported (incl., amount, time, date, place of origin, etc.);
- the information about the manner of execution of the virtual currency transaction;
- other data specified in the relevant FINTRAC instructions.

The reports mentioned in this chapter shall be sent through a web reporting system or batch file transfer as explained above in accordance with Standard Batch Reporting Instructions and Specifications, Large Cash Transaction Report Specifications, Validation Rules and Forms approved by FINTRAC (annex 11).

External electronic funds transfer reports (EFTR)

The Company must submit a non-SWIFT EFT report in case of any incoming or outgoing international funds transfers no later than five working days after the day of the transmission of the instructions (through any electronic, magnetic or optical device, telephone instrument or computer) if the value of such transfers is equal to or exceeds $10,000, regardless of whether the transaction is concluded in one or more related transactions within 24 hours period. There are two types of reports to be submitted and sent to FINTRAC for the following transactions:

- outgoing transfer of EFT that requires an EFTO report;
- incoming transfer of EFT that requires an EFTI report.

The Company shall submit a SWIFT EFT that applies in case the Company sends/receives EFTs by transmission of a SWIFT MT 103 message as a SWIFT member through the SWIFT network.

The reports mentioned in this chapter shall be sent through a web reporting system or batch file transfer as explained above in accordance with Specifications for Non-SWIFT EFT reports (EFTO and EFTI), Standard Batch Reporting Instructions and Specifications, Validation Rules and Order on Forms.

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.

The data specified above which shall be entered in the electronic record (as described above) in chronological order on the basis of documents confirming a Monetary Operation or transaction or other legally valid documents related to the execution of Monetary Operations or transactions, immediately or as soon as possible after the execution of a Monetary Operation or transaction.

The storage of records data shall be completed and kept in an electronic medium (in the Company's internal system) automatically and the Company is responsible for ensuring records keeping. The records' data is be stored using software allowing for export of details stored to Microsoft Office Excel, Word, or equivalent open-code software, without damaging integrity of the details.

Data to be retained and retention terms

The data and documents related to aforementioned transactions, reports, documents and business relationship shall be retained for at least 5 years after the conduction of specific transaction or monetary operation, fulfillment of reporting obligation, conclusion of agreements or termination of the relevant Business Relationship with the relevant customer.

The time limits for record keeping may be extended additionally under the instruction of a competent authority, but the period can't be shorter than it is established.

The Company deletes the retained data after the expiry of the time period, unless the legislation regulating the relevant field establishes a different procedure or receives the instruction from competent authority to extent the retention periods. The deletion of data is responsibility of the Compliance Officer.

Training

The Company ensures that its employees (incl., agents or mandataries, or other persons authorized to act on your behalf) have the relevant qualifications for their work tasks. When the employee is recruited or engaged, the qualifications are checked as part of the recruitment/appointment process.

In accordance with the requirements applicable to the Company on ensuring the suitability of the employees, the Company makes sure that such employees receive appropriate training and information on an ongoing basis to be able to fulfil the Company's obligations in compliance with the applicable legislation. It shall be ensured through training that the employees are knowledgeable within the area of AML/CTF to an appropriate extent considering the Employee's tasks and functions. The employees of the Company need to acknowledge the following:

- rules and requirements under the ML/TF Act of Canada and other Regulations;
- definitions and methods of ML/TF;
- importance of contribution into ML/TF activities;
- compliance policies and procedures (incl., risk assessment, CDD requirements, enhanced measures and record keeping);
- roles and responsibilities relating to the detection of ML/TF activities.

The training is structured on the basis of the risks identified through the Company's risk assessment. For new Employees, the training consists at least of a review of the content of the applicable rules and regulations, the Company's internal policies (incl. this Program) and other relevant procedures.

The content and frequency of the training is adapted to the employee's tasks and function on issues relating to AML/CTF measures. If this Program and/or any of its annexes are updated or amended in some way, the content and frequency of the training is adjusted appropriately.

The Compliance Officer shall make a **training plan (annex 13)**, which should contain at least the following details:

- training recipients:
  - front-line staff or agents;
  - employees involved in transaction operations;

    - employees responsible for cash, funds or virtual currency;
    - employees responsible for compliance program (incl., compliance officer, senior management, information technology staff or internal auditors);
- training topics and materials;
- training methods and delivery:
    - self-directed learning;
    - information sessions;
    - meetings, classrooms or conferences;
    - on-the-job training;
- Training frequency:
    - regular;
    - upon the specific event.

The Company shall institute and document the training plan in writing for the ongoing training program implementation. The training program shall cover the aforementioned details, as well as the description on how the training plan will be implemented (incl., timeline, employee engagement, learning goals, and related resources). Participant progress shall be monitored during training to ensure the program is effective.

FINTRAC shall examine and verify the compliance with the requirement to develop and maintain a written ongoing training plan for employees or agents. In course of such examination, FINTRAC uses the following methods:

- examines the scope of training recipients, covered topics, implementation and delivery of training plan;
- verifies the adequacy of training plan and approves it taking into account the size, type, nature and complexity of the business.

The training held must be documented electronically and confirmed with the employee's signature on the training protocol (annex 14). This protocol should include the content of the training, names of participants and date of the training.

In addition to the above, the employees are kept informed by the Compliance Officer on an ongoing basis about new trends, patterns and methods and are provided with other information relevant to the prevention of ML and TF.

Review of the Compliance Program

The performance of this Program shall be reviewed by the Auditor in order to ensure effectiveness of the Compliance Program (hereinafter – Effectiveness Review). The Auditor must have the required competency, tools, and access to the relevant information in all structural units of the Company. If there is no auditor, the review shall be conducted by a person, who is knowledgeable of ML/TF requirements under the applicable legislation and associated regulations, and who is directly involved in Compliance Program activities.

The Auditor must carry out the Effectiveness Review at least every two years (at a minimum) in accordance with the Effectiveness Review plan, that shall cover at least the following fields:

- the Company´s policies and procedures;
- the Company´s risk assessment;
- the Company´s training program.

The Auditor shall apply specific measures in order to detect weaknesses in the Compliance Program, which can include:

- interviews with staff who is engaged in handling transactions;
- the review of documentation (incl., procedures and policies for identification, risk assessment etc.);
- the review and sampling of records (incl., high-risk clients, transactions, reports).

The extended list of Effectiveness Review measures is located in a separate document (annex 15). The exact measures for performing Effectiveness Review shall correspond to the Company's size and their nature, scope and level of complexity of the activities and services provided. The Auditor must consider at least examination fields specified above. The Effectiveness Review shall be performed no later than 24 months from the start of the previous review, whereas the latest must be completed.

The results of Effectiveness Review measures implementation (hereinafter in this chapter – the Review Data) shall be documented and saved separately from other data and retained within 5 years. The persons who have access to the Review Data must not disclose it to anyone without prior consent of the CEO.

The Review Data shall be saved in chronological order with format, which allows to analyze this and understandable connect this to other relevant data.

In case of an entity, the Auditor must report, in writing, to the Compliance Officer within 30 days after the completion of the Effectiveness Review at least the following:

- the results of the review (incl., recommendations, deficiencies, action plans);
- the updates made to the Company´s policies and procedures in course of reporting period;
- the status of the implementation of the updates aforementioned.

FINTRAC examination of the Compliance Program

FINTRAC verifies that the Company conducts the Effectiveness Review of their policies and procedures, risk assessment and training program every two years. The purpose of FINTRAC examination is to verify that the Company's Effectiveness Review is adequate regarding the size, nature and complexity of the business, as well as consistent with the risk assessment.

In course of such examination, FINTRAC may

- review the plan of Effectiveness Review;
- review the policies and procedures;
- review the scope and methodology of the Effectiveness Review;
- assess the implementation of the Compliance Program;
- identify areas with unfulfilled requirements.

Annexes

Annex title	Document description
1. Resolution of approving the AMLCTF Compliance Program	The Company´s CEO´s draft for approving this AMLCTF Compliance Program
2. Services Description	Describes the services provided by the Company.
3. List of Risk Factors	List of risk factors which are used for determination of the customer's risk profile.
4. Customers' Onboarding Procedure	Description of the procedure which shall be applied in the case the customer shall pass the onboarding procedure.
5. Reliable Sources of Information for Dual-process Method	List of reliable sources for different categories of information that can be used for verification of customer´s identity.
6. Beneficial Owner Identification Guidelines	Description of principles for the customer's beneficial owner identification.
7. Procedure for Application of EDD Measures	Describes EDD measures which shall be applied to the high-risk customers.
8. Requirements for Transactions Monitoring	List of ODD measures which shall be applied by the Company for the monitoring of transactions.
9. Indicators of Suspicious Activities and Transactions	List of potential red flags that could initiate suspicion of ML or TF and indicate irregularities related to financial transactions or attempted transactions.

10. Internal Report Form	Internal reporting form which should be filled by the Onboarding Specialist and/or Monitoring Specialist when notifying the Compliance Officer
11. External Report Forms	External reporting forms for STR,TPR, LCTR/LVCTR, EFTR to be submitted and sent to FINTRAC.
12. Validation Rules	List of validation specifications for submission of reports to the FINTRAC and description of further actions.
13. Training plan	Written training plan document that sets out the training recipients, strategies, curriculum, and methods for training employees across the Company.
14. Training Protocol	Form which should be signed if the Employee has passed the relevant training.
15. Effectiveness Review measures	The list of measures the auditor shall take in course of two-year Effectiveness Review.

Version Control Table

Approval date	Changes description
dd.mm.yyyy	First issue