CONFIDENTIAL

Vidia

Anti-Money Laundering and Counter Terrorist Financing Policy

2025

Document owner
Money Laundering Reporting Officer

Document maintenance
Money Laundering Reporting Officer

Approval	Version	Date of approval
Management	1.0.	August 25, 2025

Contents

1. INTRODUCTION

Vidia Corporation Inc. (hereinafter: the Company), registered on August 9th, 2024, in Alberta Corporate Registry under business number (BN) 718343957) and incorporation no 2026373585 provides money transferring, virtual currency and PSP services as of September 26th, 2024, when duly registered in Money Service Business Registry of Canada under MSB registration number C100000225.

The Company functions as a money services business (hereinafter: MSB) with inherent responsibility for processing its merchant clients' transactions.

By undertaking its MSB responsibilities The Company recognizes its increased exposure money laundering and terrorist financing risks and assumes a moral, social and legal obligation to proactively mitigate inherent risk.

With adoption of Anti-Money Laundering and Counter Terrorist Financing Policy (hereinafter: AMLCTF Policy), the Company adopts a fundamental anti-money laundering and counter terrorist financing (hereinafter: AMLCTF) set of rules for the provision of MSB services.

AML Policy acknowledges the role of the Company as AMLCTF obliged entity, defines legal framework to which it adheres and prescribes key pillars for the provision of efficient and effective AMLCTF program, defining core principles, structure, rules and responsibilities for each pillar.

AMLCTF Policy therefore serves as umbrella document in alignment with which other operative procedures are proposed and adopted.

2. REGULATORY FRAMEWORK

All AMLCTF measures and procedures adopted by the Company are based on the regulatory framework of Canada which has a foothold in international standards adopted by Financial Action Task Force (hereinafter: FATF).

The Company adheres to Canadian legislation, but also when needed applies stricter AMLCTF standards, if such approach is required by the Company stakeholders located or related with other jurisdictions.

2.1. INTERNATIONAL REGULATORY FRAMEWORK

The FATF Recommendations: International Standards on combating money laundering and the financing of terrorism;[1]

Compliance with United Nations Security Council Resolutions is regulated as mandatory in Canada, and therefore the Company adheres to *United Nations Security Council Consolidated List*[2] during regular sanction checks.

Although compliance with United States of America and EU sanctions programs are not mandatory for MSBs registered and regulated in Canada, considering their global impact and reach the Company adheres to sanction program adopted by the Office of Foreign Assets Control of US Department of Treasury, in particular *Specially Designated Nationals and Blocked Persons List (hereinafter: SDN List*) and Consolidated *Non- Specially Designated Nationals List (hereinafter: Non- SDN List)*[3] and sanction programs adopted by European Commission with the *Consolidated EU Sanction List*[4].

If in the course of ongoing restriction measures controls the Company comes to knowing that its client or other persons connected with the client are enlisted by some other international sanction program that is not deemed as mandatory by Canada, upon client risk assessment the Company may decide to take more stringent approach towards such client in accordance with the Client Due Diligence and Sanctions Procedure.

1 FATF Recommendations 2012-2025

2 https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list

3 https://sanctionssearch.ofac.treas.gov/

4 https://www.sanctionsmap.eu/#/main

2.2. NATIONAL REGULATORY FRAMEWORK OF CANADA

The Company adheres to following national legislation[5] [6] when establishing AMLCTF principles and measures in the scope of the registered MSB activities:

- Criminal Code (R.S.C., 1985, c.C-46);
- Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c.17);
- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (SOR/2002-184);
- Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transactions Reporting Regulations (SOR/2001-317);
- Financial Transactions and reports Analysis Centre of Canada Assessment of Expenses Regulation (SOR/2023-195);
- Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulation (SOR 2007-292);
- United Nations Act (R.S.C., 1985, c. U-2);
- Special Economic Measures Act (S.C. 1992, c. 17) with all by related Regulations;
- Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law) (S.C. 2017, c. 21) with all related Regulations;
- Freezing Assets of Corrupt Foreign Officials Act (S.C. 2011, c.10) with all related Regulations;
- Consolidated Canadian Sanctions List;[7]

[5] AMLCTF Regulation in Canada

[6] Sanction legislation, Canada

[7] Consolidated Canadian Sanctions List

3. BASIC TERMS

Bearer share is equity security wholly owned by the person or entity that holds the physical stock certificate. The issuing firm neither registers the owner of the stock nor track transfers of ownership. The company disperses dividends to bearer shares when a physical coupon is presented to the firm. Considering that the share is not registered by any authority, transferring the ownership of the stock involves only delivering the physical document.

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

- that involves the beneficiary withdrawing cash from their account;
- that is carried out by means of a direct deposit or a pre-authorized debit;
- that is carried out by cheque imaging and presentment;
- that is both initiated and finally received by persons or entities that are acting to clear or settle payment obligations between themselves; or
- that is initiated or finally received by AMLCTF obliged person or an entity for the purpose of internal treasury management, including the management of their financial assets and liabilities, if one of the parties to the transaction is a subsidiary of the other or if they are subsidiaries of the same corporation.

Embargo is the order of government and/or international and regional bodies that introduces restrictions to the trade or the exchange of goods and services with a specific country. Embargo usually arises because of unfavorable political and economic circumstances among nations. The aim of the embargo is to isolate the country in relation to which unfavorable political or economic circumstances have been identified, and thus to create difficulties in managing a specific country to force the governing body of the country concerned to act to resolve problematic circumstances.

Fiat currency means a currency that is issued by a country and is designated as legal tender in that country.

Fictive bank is a bank not physically present in the country where it is founded and licensed, nor is it a member of a financial group that is subject to effective, consolidated supervision. Physical presence in this sense means that decision-makers and managers have a place of residence or whereabouts within the state.

Financial Action Task Force (FATF) is an international organization founded in 1989 on the initiative of G7, with the aim of developing international AML standards and policies. In 2001, FATF's activities have been extended to the development of standards and policies of counter terrorist financing. The FATF regularly revises recommendations related to AMLCTF controls the compliance of national AMLCTF systems in accordance with the recommendations.

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is Canada's financial intelligence unit and anti-money laundering and anti-terrorist financing supervisor. Its mandate is to facilitate the detection, prevention and deterrence of money laundering and the financing of terrorist activities, while ensuring the protection of personal information under its control.

Foreign currency means a fiat currency that is issued by a country other than Canada.

Foreign currency exchange transaction means an exchange, at the request of another person or entity, of one fiat currency for another.

Funds means

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

For greater certainty, it does not include virtual currency.

Information record means a record that sets out the name and address of a person or entity and

- in the case of a person, their date of birth and the nature of their principal business or their occupation; and
- in the case of an entity, the nature of its principal business.

Initiation, in respect of an electronic funds transfer, means the first transmission of the instructions for the transfer of funds.

International electronic funds transfer means electronic funds transfer other than for the transfer of funds within Canada.

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

- the date of the receipt;
- if the amount is received for deposit into an account, the name of each account holder;
- the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
- the type and amount of each virtual currency involved in the receipt;

- the exchange rates used and their source;
- the number of every other account that is affected by the transaction, the type of account and the name of each account holder;
- every reference number that is connected to the transaction and has a function equivalent to that of an account number;
- every transaction identifier, including the sending and receiving addresses; and
- if the amount is received by a dealer in precious metals and precious stones for the sale of precious metals, precious stones or jewelry,
  - the type of precious metals, precious stones or jewelry,
  - the value of the precious metals, precious stones or jewelry, if different from the amount of virtual currency received, and
  - the wholesale value of the precious metals, precious stones or jewelry.

Money laundering is a criminal offence meaning:

1. replacement or transfer of property, when it is known that such property is acquired through criminal activity or participation in a criminal activity in order to hide or conceal the unlawful origin of the property or to assist any person involved in the perpetration of such an activity in avoiding the legal consequences of that person's actions;
2. hiding or concealing the true nature, sources, location, disposal, movements, rights associated with the ownership or ownership of the property, when it is known that such property is acquired through criminal activity or participation in such activity;
3. acquisition, possession or use of property, if it is known, at the time of receipt, that such property has been acquired through criminal activity or by participating in such activity;
4. participation, association for the purpose of committing or attempting to commit a criminal offence and assisting the perpetrator, encouraging, favouring and counselling at the commencement of any of the activities referred to in items 1, 2 or 3 of this definition.

Offshore financial centre or tax haven is a country or jurisdiction providing financial services to non-residents to an extent that is not proportionate to the size and financing of the domestic economy of the respective country or jurisdiction. Consistent with the proposed definition, the basic indicator of OFC country status or jurisdiction is determined through the level of net exports of financial services in relation to gross domestic product.

Offshore centres are all financial centres or special zones offering liberal regulations in conducting financial transactions.

The basic characteristics of OFCs can be summarized as follows:

- primary business orientation is dealing with non-residents;
- a simple and inexpensive process of establishing a legal entity;
- poor supervisory standards, minimum requirements in terms of financial reporting;
- low or zero tax burden;
- non-compliance with international standards for anti-money laundering and counter terrorist financing.

Offshore company is a legal entity registered in an offshore financial center or tax haven, established, and operating according to the benefits provided by offshore financial centers.

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

- enables a person or entity to access a credit or debit account or one that is issued for use only with merchants; or
- is issued for single use for the purposes of a retail rebate program

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

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

Receipt of funds record means a record that indicates the receipt of an amount of funds and that contains the following information:

- the date of the receipt;
- if the amount is received from a person, their name, address and date of birth and the nature of their principal business or their occupation;
- if the amount is received from or on behalf of an entity, the entity's name and address and the nature of its principal business;
- the amount of the funds received and of any part of the funds that is received in cash;
- the method by which the amount is received;
- the type and amount of each fiat currency involved in the receipt;
- if applicable, the exchange rates used and their source;

- the number of every account that is affected by the transaction in which the receipt occurs, the type of account and the name of each account holder;
- the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
- every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
- the purpose of the transaction.

Senior officer, in respect of an entity, means

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

Shell company is a legal entity with no significant assets and real business used exclusively as a means of conducting business transactions not related to an actual business activity of a legal entity, but are mainly related to attempts of fraud, tax evasion and money laundering.

Suspicious transaction is any transaction for which the Company estimates that there are reasons and circumstances that raise MLTF suspicion, or that the transaction involves funds derived from illegal activities.

SWIFT means the Society for Worldwide Interbank Financial Telecommunication.

Terrorist financing is a criminal offence[8] that involves the provision or collection of the funds, or an attempt to ensure or collect funds, whether legal or illegal, in any way, directly or indirectly, with the intent to use them or knowing that they will be used, in whole or in part, by a terrorist or a terrorist organization for any purpose, including the commission of a terrorist offence or by the persons who finance terrorist acts.

Virtual currency means

- a digital representation of value that can be used for payment or investment purposes, that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or

[8] International Convention on Counter Terrorist Financing (Official Gazette – International Agreements 16/03)

- a private key of a cryptographic system that enables a person or entity to have access to a digital representation of value

Virtual currency exchange transaction means an exchange, at the request of another person or entity, of virtual currency for funds, funds for virtual currency or one virtual currency for another. ()

Virtual currency exchange transaction ticket means a record respecting a virtual currency exchange transaction — including an entry in a transaction register — that sets out

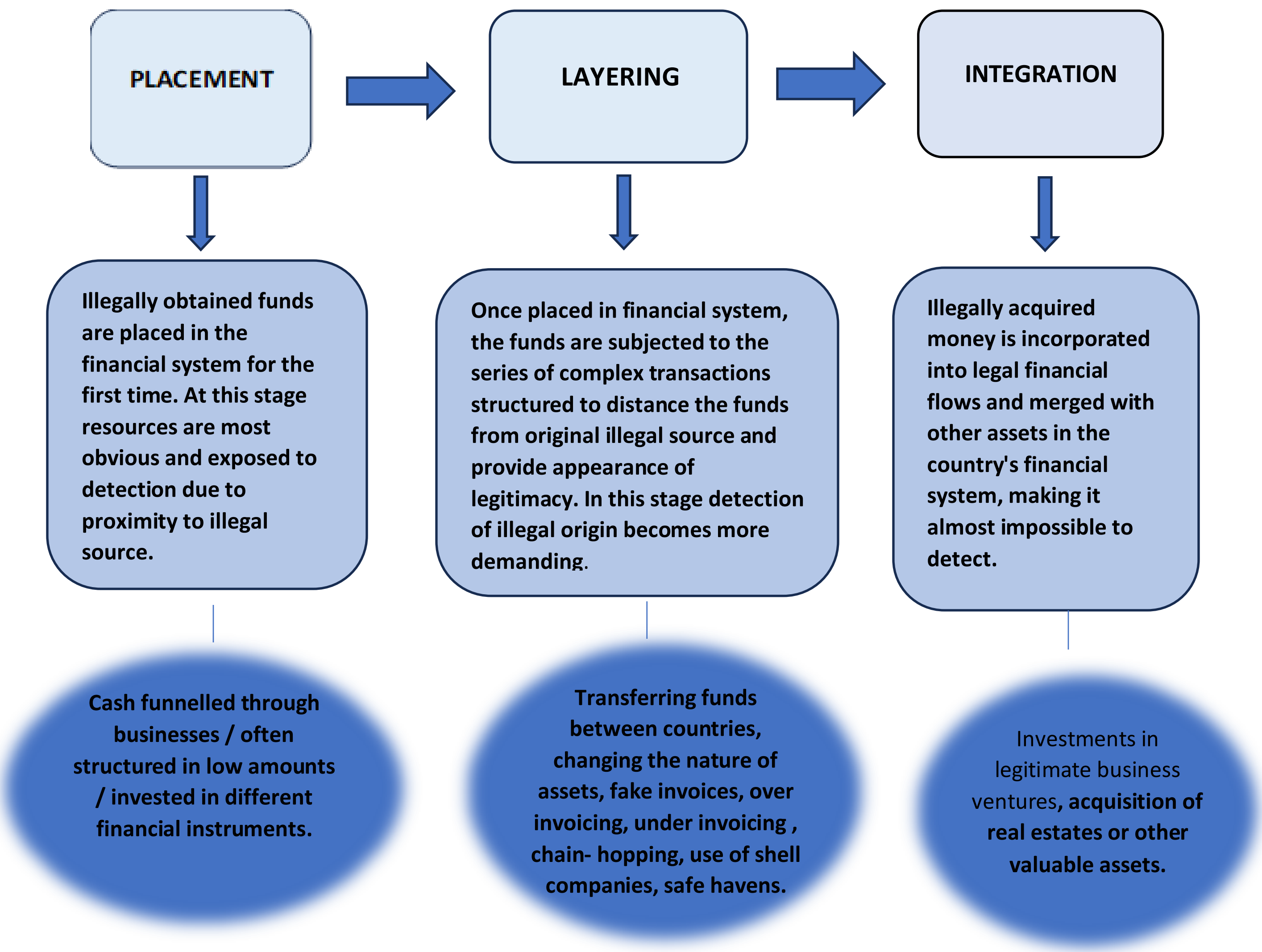
- the date of the transaction;
- in the case of a transaction of $1,000 or more, the name and address of the person or entity that requests the exchange, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
- the type and amount of each type of funds and each of the virtual currencies involved in the payment made and received by the person or entity that requests the exchange;
- the method by which the payment is made and received;
- the exchange rates used and their source;
- the number of every account that is affected by the transaction, the type of account and the name of each account holder;
- every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
- every transaction identifier, including the sending and receiving addresses.

4. DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Money laundering detection process

To freely use illegally acquired funds and motivated by the desire not to get caught by law enforcement, criminals aim to falsely present the illegally obtained money as legitimately acquired.

With aim to display a veil of legitimacy over illegally obtained funds they engage in the process of money laundering, which is generally recognized to take place through 3 stages.



Financing of terrorism detection process

Financing of terrorism detection process is demanding given that terrorism, unlike money laundering, may be financed from legitimate sources or self-financed, amounts are generally smaller, and transactions often take place outside formal financial system.

On instances when terrorism is financed from illegal activities, such as narcotics or precious metal trade, extortion, financial fraud, methods used for detection of money laundering may be used to detect financing of terrorism as well.

In other cases, financial institutions use sanction list screening and KYC verifications as a method of detection.

Comparison: money laundering vs. financing of terrorism

FEATURES	MONEY LAUNDERING	TERRORIST FINANCING
MOTIVATION	PROFIT	IDEOLOGICAL ORIENTATION
SOURCE OF FUNDS	INTERNALLY, BY CRIMINAL ORGANIZATION ITSELF	INTERNALLY, AUTO-FINANCING BY THE CELLS, EXTERNALLY BY VARIOUS FINANCIERS
IMPLEMENTATION ENVIRONMENT	FORMAL FINANCIAL SYSTEM	COMPANIES FOR ORGANIZATION OF CASH TRANSFERS, NON-PROFIT ORGANIZATIONS, GAMING PLATFORMS, UNDERGROUND FINANCIAL SYSTEMS - HAWALA
FOCUS AT DETECTION	SUSPICIOUS TRANSACTIONS, NON-CHARACTERISTIC DEPOSITS CONSIDERING CLIENT'S ASSETS AND EXPECTED ACTIVITY	SUSPICIOUS RELATIONSHIPS, TRANSACTIONS CONDUCTED BETWEEN PERSONS NOT CONCTED LEGALLY OR FINANCIALLY
TRANSACTION AMOUNTS	HIGH, OFTEN STRUCTURED IN SMALLER AMOUNTS TO AVOID REPORTING OBLIGATIONS	SMALL AMOUNTS, MOSTLY BELOW THE REPORTING THRESHOLDS
FINANCIAL ACTIVITY	COMPLEX TRANSACTIONS ARRAYS THAT OFTEN INCLUDE MULTIPLE JURISDICTIONS, OFFSHORE COMPANIES, TAX HAVENS	NO PARTICULAR TYPE
MONEY FLOW	CIRCULAR- FUNDS ARE RETURNED TO THE PERSON WHO GENERATED THEM	LINEAR – GENERATED FUNDS ARE USED FOR TERRORIST MEANS

5. AMLCTF ORGANIZATION SYSTEM

The Company as a subject in the national AMLCTF organization system of Canada

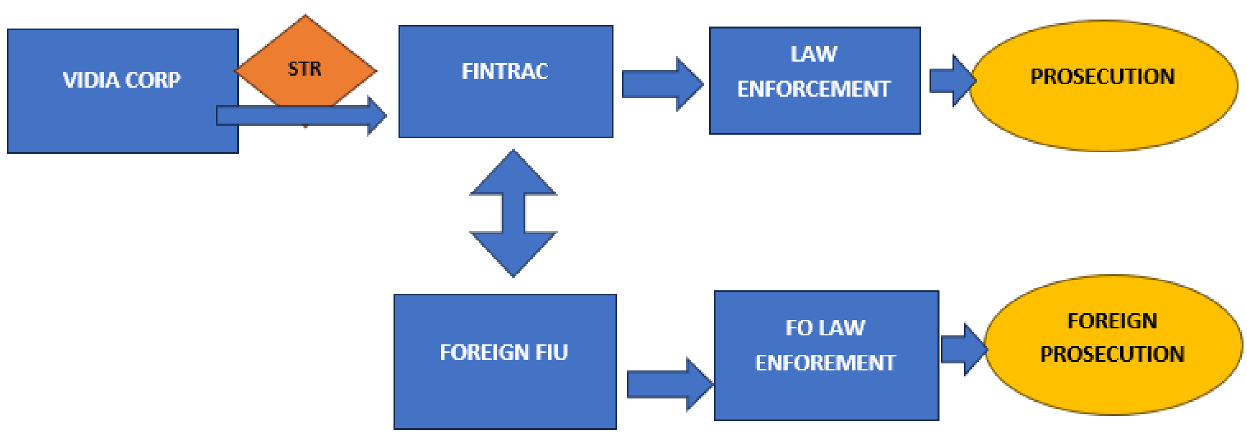
As a Money Services Business (MSB) registered in Canada, the Company offers money transfer, payment service provider (PSP), and virtual currency services to its clients. In accordance with Canadian legislation, the Company is designated as an AML/CTF obliged entity, requiring the implementation and execution of preventative measures across all client interactions, transactions, products, and services.

This role carries the privilege of contributing to national and global efforts to combat financial crime.

The primary objective of these AML/CTF measure detailed in subsequent sections of this Policy with respect to their type, purpose, scope, frequency, and assigned responsibilities **is** to detect and report suspicious transactions or activities within the Company's operations to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)**.**

Upon submission of a Suspicious Transaction Report (STR)**,** FINTRAC evaluates the findings and, where warranted, escalates the matter to Canadian law enforcement authorities for potential legal action. In cases involving foreign residents or entities, FINTRAC may share the STR with the relevant foreign financial intelligence unit (FIU)**,** enabling further investigation within the applicable legal framework of that jurisdiction.

Similarly, when client activities occur outside Canada, foreign financial intelligence units (FIUs) may share information about suspicious client behavior with FINTRAC.



5.1. INTERNAL AMLCTF PROGRAM – KEY PILLARS

1. Governance

Definition and implementation of 3 lines of control roles and responsibilities under the Management governance.

2. Policies and Procedures

Definition of the structure of internal policies and procedures, creation, updates and adoption roles and responsibilities.

3. AMLCTF Control Processes

Definition of key AMLCTF control processes: MLTF Risk Analysis and Assessment, Client Due Diligence, Sanctions program, manner and responsibilities related to their implementation.

4. Efficiency Controls and Audit

Definition and implementation of AMLCTF efficiency controls and regular audit which guarantee the effectiveness of control implementation.

5. Reporting

Definition of the rules, roles and responsibilities regarding internal and FINTRAC reporting.

6. Training and Awareness

Manner of conduction and periodicity for regular and role specific trainings.

7. Data Record Keeping

Manner, duration, roles and responsibilities regarding data record keeping.

6. GOVERNANCE

Management of the Company is committed to the culture of compliance and by setting the tone from the top it ensures that AMLCTF measures are ingrained in everyday operations, not just treated as regulatory checkbox.

Management determines to position compliance as a shared responsibility across all business lines and encourages each employee to acknowledge, adopt and raise awareness of its own irreplaceable role in the compliance process, being aware that only when compliance is prioritized as a core value, and not just a legal obligation the Company can innovate responsibly while maintaining trust with regulators and customers.

To enhance and boost AMLCTF compliance system the Company implements 3 lines of defence that are under direct competence of the Management.

a) First line of defence

First line of defence has the primary responsibility to own and manage risks associated with day-to-day operation activities.

Owners of this line of control are the employees of organizational units that maintain immediate contact with the client in the onboarding process, that is, sales and customer support.

First line of defence provides AMLCTF controls in accordance with the specifications within operational procedures is stipulated under chapter 7. of this AMLCTF Policy.

b) Second line of defence

Second line of defence enables the identification of emerging risks in daily business operation. It does so by providing compliance and oversight in the form of definition of policies and procedures, implementation of key process controls, provision of efficiency controls, compliance incentives to Management and reporting about efficiency control outcomes, AMLCTF project management, statutory FINTRAC reporting, training and awareness, cooperation with Internal Audit and the authorities.

Owner of the second line of control is Money Laundering Reporting Officer (hereinafter: MLRO) and MLRO deputy at times of MLRO absence.

MLRO provides second line of control as autonomous function, independent and not subordinated to other business lines, directly reporting to Management.

Before the MLRO appointment, designated units that provide human resources controls should ascertain that the MLRO has adequate AMLCTF experience in the financial system, no pending criminal proceedings and no prior criminal offence convictions.

Acceptable verification methods for performing these checks are CV collection, references from reliable sources, collection of updated impunity statements (not older than a month) and adverse media checks.

c) Third line of defence

Third line of defence provides control of the AMLCTF activities both first and second line of defence with aim to detect potential irregularities or illegalities in the implementation and provision of AMLCTF controls.

Owner of the third line of defence is internal audit which can be outsourced for the provision of regular and mandatory annual AMLCTF system controls or on occasion when needed, as well for the provision irregular AMLCTF system controls.

When developing the audit program, it is ensured that the program is aligned with the size and scope of the Company's business, risk profile, ML/CFT risk exposure and adjusted to the specifics of the Company's AML/CFT system.

Designated auditor provides audit outcomes in the form of the report submitted to the Management. Submitted report indicates deficiencies, irregularities or illegalities and provides proposals for mitigation measures in the form of recommendations with designated deadlines.

Designated auditor must have a valid audit certificate issued in the resident country.

d) Management responsibilities

The Management of the Company is responsible for establishing and overseeing an effective AMLCTF compliance program, always ensuring its regulatory adherence, risk mitigation, operational integrity and coherence, through the provision of the following measures:

- Establishment an appropriate and effective organizational and operational structure necessary for compliance with the AMLCTF strategy, paying special attention to sufficient authority and the adequacy of human and technical resources assigned to MLRO;
- Adoption AMLCTF policies, controls, and procedures and ensure their implementation;
- MLRO appointment;
- Ensuring that the MLRO holds a position within the organizational structure that allows them to perform their AML/CTF duties promptly, effectively, and independently, with direct communication access to the Management;

- Ensuring that MLRO deputy has unrestricted access to all necessary data, information, and documentation and adequate working conditions;
- Ensuring MLRO suitable physical and technical conditions that guarantee an adequate level of confidentiality for the data and information they handle;
- Implementation of a system that enables the Company and MLRO to promptly and securely submit all requested data, information, and documentation to FINTRAC and supervisory authorities, ensuring data protection;
- Ensuring regular professional training and education for the Company's employees;
- Implementation of efficient and effective line control system;
- Maintenance of effective communication and cooperation, including proper information flow across all organizational levels of the Company;
- Review the MLRO activities at least once a year;
- Establishment of an appropriate information system, considering the Company's organizational structure and business scope, volume and exposure to MLTF risks.

7. AMLCTF POLICIES AND PROCEDURES

The function of AMLCTF Policy is to provide formal rules for implementation of key pillars of AMLCTF program, acknowledged across the organization upon their adoption.

Upon AMLCTF Policy adoption, AMLCTF Procedures are designated to further elaborate operational aspects of key pillars of AMLCTF program such as to provide step-by-step instructions related to the manner of risk assessment and management of risk exposure and guidelines on the AMLCTF measures undertaken by the employees during the provision of their day-to-day AMLCTF activities.

The Company implements following Policies and Procedures:

AMLCTF POLICY

High – level framework that outlines the Company's AMLCTF commitments and objectives.

Defines basic principles of AMLCTF program: method of governance, key control processes and reporting postulates, rules related to training and awareness and record keeping.

MONEY LAUNDERING AND TERRORIST FINANCING RISK ANALYSIS AND ASSESSMENT PROCEDURE

Defines the procedure for MLTF risk analysis and assessment both at the level of the Company and at the level of an individual client.

Determines what is analysed and assessed and who, when and how performs risk analysis and assessment.

By determining risk levels provides input for implementation of client due diligence measures.

CLIENT DUE DILIGENCE AND SANCTIONS PROCEDURE

Provides know your client (KYC) and ongoing monitoring and screening procedure in a manner that is proportional to the MLTF risk assessment.

Determines who, when, what, how performs the client check during onboarding and ongoing monitoring and screening.

AMLCTF policy and procedures are proposed by MLRO, accordingly with the risk appetite input provided by the Management.

MLRO prepares policies and procedures reviews and /or updates with the implementation of every change of the regulatory framework which affects AMLCTF processes of a Company, with every change of business scope or implementation of new business functionalities and services, or at least once a year.

Policies and procedures are formally adopted by the Management of the Company and duly brought to the attention of all employees within the organization who are required to adhere to the procedures and apply them in their AMLCTF day-to-day activities.

8. AMLCTF CORE PROCESSES

8.1. RISK BASED APPROACH (RBA)

AMLCTF controls provided by the Company are summoned around 2 core processes:

- Money laundering and Terrorist Financing Risk Analysis and Assessment;
- Client Due Diligence and Sanctions.

Objectives of these 2 processes can be achieved fully only with application of complementarity and proportionality principles.

MLTF Risk Analysis and Assessment, targeted either at Company-wide or client-based assessment, will not achieve its optimal efficiency unless not accompanied by implementation of qualitatively proportional Client Due Diligence and Sanctions measures structured in series of controls aiming to obtain knowledge about the client's profile, so Company can be able to reduce MLTF risk that manifests through the client's use of products and services.

The advantage of the risk-based approach that applies proportionality when implementing risk mitigation measures is in using available resources in accordance with the priorities.

Operationally this means that the Company will pay more due diligence to the clients assessed with high risk than to those assessed with lower ranks.

Broader scope of due diligence intended for high-risk clients pertains to gathering more substantial information scope to produce more reliable client verification outcomes and to conduction of more frequent high-risk client reviews.

Implementation of risk-based approach provides several benefits for the Company such as:

- ✓ Efficient use of resources, which implies reducing the claims for wider documentation range from the entire client base;
- ✓ Adoption of flexible approach tailored to the specific risks and business activity of the organizational structure;
- ✓ Orientation to a high-risk category complicates MLTF use of financial system.

RBA adoption requires implementation of following process elements:

- ✓ Identification and analysis of risk criteria and risk factors;
- ✓ Definition of risk assessment methodology in the terms of factor pondering and criteria categorization and ongoing assessment updates;
- ✓ Establishment of Company-wide AMLCTF preventative system and client-oriented set of CDD controls proportional with risk assessment outputs.

8.2. RISK ANALYSIS AND ASSESSMENT PRINCIPLES

MLTF Risk Analysis and Assessment is the core measure of MLTF prevention because it provides inputs for the scope of risk mitigation measures.

Process of risk analysis should include 4 criteria:

- Client risk;
- Country risk;
- Product risk;
- Delivery channel risk;

and identify and analyse specific risk factors pertaining to each criteria in comparison with the scope of the Company's business plan and program.

Scope of client risk criteria analysis includes at least following factors:

- Credibility of client or the client's UBO;
- Politically exposed person status;
- Sanction / Enforcement list inclusion;
- Client and UBO reputation;
- Organization structure;
- Business activity;
- Transparency of ownership and complexity of the ownership structure;
- Information on submission STR report related to the client;

- Information on funds blockade due to administrative or criminal proceedings.

Scope of country risk criteria analysis includes at least following factors:

- Countries included on the FATF black and grey lists;
- Countries under embargo or countries known as sponsors of terrorism;
- Offshore centres;
- Level of corruption perception;
- Level of predicate offences;
- Countries assessed as high risk by EU delegated act;
- Level of tax transparency;
- Membership with FATF or FATF-style body;
- Countries with AMLCTF legislation equivalent to Canada.

Risk factors for country risk should be analysed using credible and reliable sources of information, mostly referring to the reports from credible international institutions and authorities.

Scope of product risk criteria analysis includes at least following factors:

- Possibility of payment receipts from unknown and unrelated third parties;
- Product transparency;
- Product complexity;
- Product volumes;
- Established thresholds;
- Financing methods;
- Usability, transferability and monetization.

Scope of delivery channel risk criteria analysis includes at least following factors:

- Non-face-to-face onboarding application;
- Level of safeguarding measure application during non-face-to face onboarding;
- Level of misrepresentation and identity theft prevention measures;
- Third party onboarding provision;
- Agent onboarding provision.

The purpose of MLTF risk analysis and assessment process is to understand its risk exposure and determine its acceptable level of risk tolerance while assessing the risk of individual criteria by classifying them into specific categories: low, medium, increased and high risk.

During criteria risk assessment determines ponders for each analysed factor, and ensures that:

- Pondering is not influenced by a single factor, and that economic or profit considerations do not influence risk assessment;
- Pondering does not lead to a situations where it would become impossible for any business relationship to be classified as high-risk;
- Circumstances which pose a high-risk accordingly with national legislation provisions cannot be excluded by pondering;
- Automatically generated risk assessment can be overridden automatically with adequate reasoning.

When deemed necessary MLRO informs the Management of the results of both Company-wide and individual risk assessment, and in cases of high risk provides proposals for risk mitigation.

On instances when Management decides not to act in accordance with MLRO proposals, the Management duly documents its decisions and provides own mitigation measures.

The Company should not introduce new products and services or change existing products and services, enter new markets or undertake new activities until appropriate resources are available and successfully engaged to understand related MLTF risks.

Principles provided in this chapter the Company considers when preparing and updating *MLTF Risk Analysis and Assessment Procedure.*

8.3. CLIENT DUE DILIGENCE AND SANCTONS PRINCIPLES

Client due diligence (hereinafter: CDD) and Sanctions is a process that begins prior to the establishment of business relationship and is carried out throughout its duration.

This process is based *know your customer* principle (hereinafter: KYC) and is applied in quantitative and qualitative proportion with client's risk assessment.

CDD / Sanctions process is applied in 2 stages:

- KYC / Sanctions verifications during onboarding process;
- Ongoing monitoring of clients' business activity and regular KYC / Sanctions reviews aligned with RBA

a) KYC / Sanction verifications during onboarding process

During this stage of CDD / Sanctions process the Company conducts face-to-face identity verification of the client and client related persons and gathers information on the purpose and intended nature of business relationship with the client.

Client is an entity with whom the Company aims to establish business relationship, while client related persons are ultimate beneficial owners, legal representatives and proxy holders of a client.

The Company conducts all relevant verifications by reviewing documents that are issued by authorities or collected from relevant public sources and as well from information provided by the client in own capacity which are duly signed.

Once all mandatory information is collected and duly verified the client will be assigned with initial risk assessment in accordance with the principles stipulated in chapter 8.2. and related MLTF Risk Analysis and Assessment Procedure.

Client assessed with low (1) and medium (2) risk will be subjected to standard CDD process.

Clients assessed with high risk (3) will be subjected to enhanced due diligence process (hereinafter: EDD) and will require formal Management approval for the establishment of business relationship.

b) Ongoing monitoring

Ongoing monitoring of clients business activity anticipates implementation of controls related to the client’s transaction volumes generated through the service client has contracted with the Company.

Ongoing monitoring controls quantitatively and qualitatively aligned with RBA, that is, in proportion with assessed client’s risk.

With implementation of ongoing monitoring controls, the Company ensures that client transaction activity related to contracted service is aligned with information obtained during KYC process such as intended nature and purpose of business relationship, source of funds and wealth, scope of business.

Provision of ongoing monitoring controls enables Company to timely detect non-compliance and mitigate the risk thereof.

During the initial month of the provision of business activities the Company will apply internal functionalities for conduction of ongoing monitoring controls.

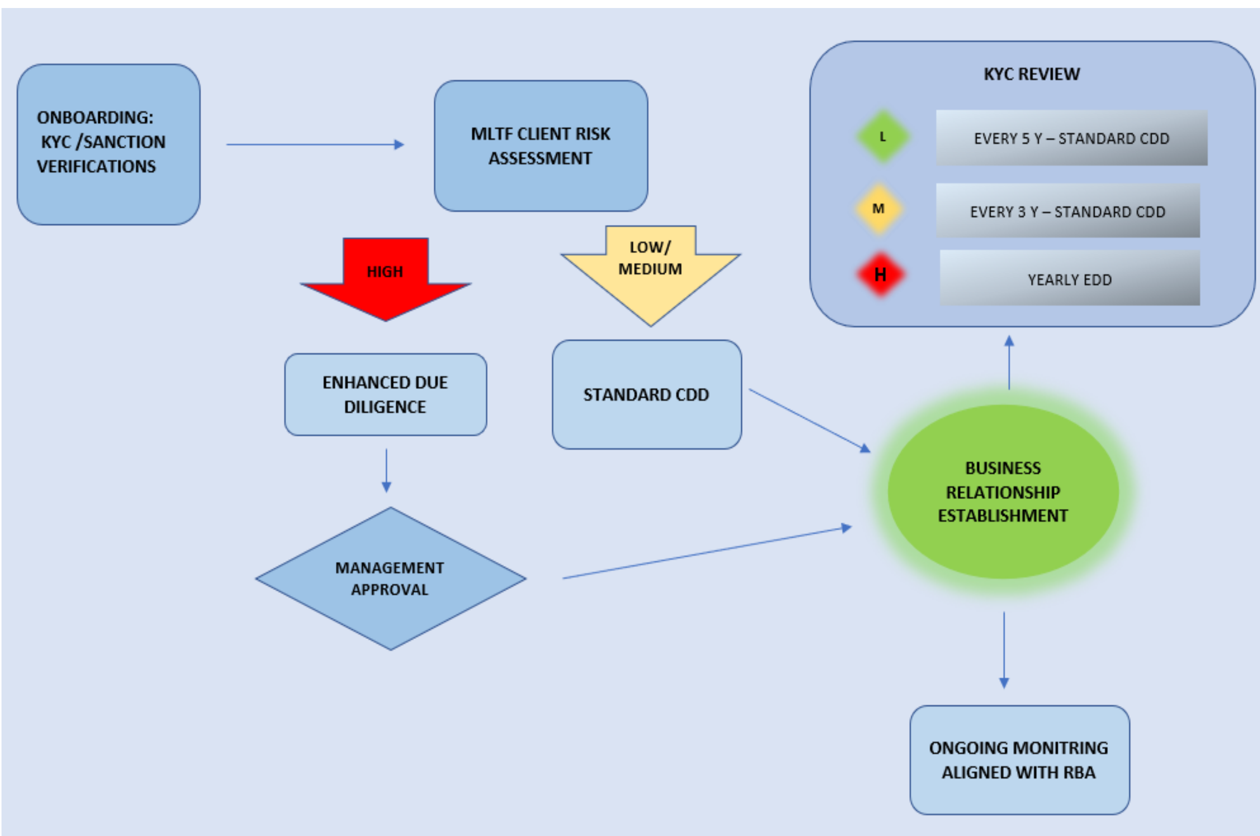
Along with enlargement of client base and increase of transaction volumes the Company will review the possibility of implementation of third-party provider transaction monitoring solution.

Throughout the duration of business relationship with the client the Company performs KYC reviews in the same scope as in onboarding process and in following periodicity: for high risk annually, for medium risk every 3rd year for low risk every 5th year and as well sanction screenings with each new update of relevant sanction lists.

Principles provided in this chapter the Company considers when preparing and updating *Client Due Diligence and Sanctions Procedure.*

The Company will not entrust the conduct of due diligence to third parties, nor will it enter contracts with agents and third parties based on a contractual relationship that implies outsourcing.

8.4. MLTF RISK ASSESSMENT AND CDD FLOWCHART



8.5. PROHIBITIONS AND RESTRICTIONS

The Company will not enter business relationship with a client in a manner that would be contrary to the international standards, governing AMLCTF laws and bylaws of Canada and applicable legislation of the countries where the Company's FI stakeholders are located.

The Company shall not accept the establishment of business relationship when following circumstances are determined:

- Identity of a client or client connected persons is not established and verified in the regulated manner;
- Client or client connected persons are sanctioned by international organizations (EU, UN, OFAC);
- Illegal business model;
- Legality of client's business model or client's source of funds cannot be ascertained;
- Clients that refuse to provide information and documentation required by the Company;
- Fictive / shell banks;
- Companies with bearer shares;
- Instances when high-risk cannot be mitigated by application of EDD measures;
- Client is resident of a country that is not stakeholder within international financial system.

The Company will act in accordance with international de-risking standards, will not exclude the whole groups of high-risk entities from possibility of establishment of business relationship, unless on instances when such approach contradicts with acceptance use policies adopted by the Company's FI stakeholders. In such cases the Company will ensure compliance with FI stakeholder's acceptance use policy throughout the duration of business relationship with such stakeholder.

On all other occasions the Company will make decisions on rejection or termination of business relationship on case-by-case basis upon appropriately convened risk assessment and after EDD controls are appropriately conducted.

9. EFFICIENCY CONTROLS AND AUDIT

a) Efficiency controls

Efficiency controls are practical steps and methods undertaken by MLRO with aim to enable the Company's compliance program to work smarter, not harder by presenting ways to cut waste, speed up checks and focus on real risks.

Efficiency controls assume quarterly testing of implemented AMLCTF system functioning with aim to measure effectiveness of implemented AMLCTF control processes, optimise resource use, improve speed, balance risk and efficiency and meet regulatory expectations.

Main areas for efficiency controls are:

- Regulatory compliance;
- Risk based approach /CDD efficiency;
- Transaction monitoring /screening;
- STR detection efficiency;
- Regulatory reporting;
- Training and awareness.

For each identified area MLRO determines Key Performance Indicators (hereinafter: KPIs) in the terms of measurable values (number/ share/ volume) that show how effectively business is achieving its objectives.

Upon KPIs measurement MLRO analyses gaps between actual results and target goals and investigates the reason for discrepancy between actual result and a target.

Once reason is determined MLRO defines measures for gaps elimination and submit reports on control outcomes with mitigation measures to the Management.

Upon Managements approval, MLRO implements approved improvements.

b) Audit

AMLCTF audit is performed by certified auditors on yearly basis or extraordinary on Management's demand.

The premise efficient AMLCTF audit is understanding of the Company's risk profile and compliance framework to ensure the audit program is tailored to actual exposures.

Auditors independently verify that policies and procedures are not only written in alignment with Company's size and business scope, but as well that implemented control system targets applicable risks effectively.

This is achieved my testing methods, such as CDD file and transaction sampling, reviewing effectiveness of suspicious activity reporting process and cross-checking data between the control systems.

Audit outcomes should be presented with clear evidence, distinguishing between minor oversights and severe compliance failures that could invite regulatory action.

The audit report must prioritize practical risk mitigation, such as updating outdated procedures, closing gaps in employee training, or recalibrating overly sensitive screening systems.

Management is responsible for implementing these changes within a defined timeframe, with auditors following up to confirm improvements are effective.

Over time, the audit process itself should evolve to address emerging risks like new money laundering typologies or changes in business operations.

10. REPORTING

AMLCTF reporting is crucial both for internal and statutory compliance because it ensures transparency and accountability at all levels.

Internal reports provide help to the Management to identify weaknesses, allocate resources effectively and demonstrate a culture of compliance to employees and stakeholders.

Statutory reports fulfil legal obligations, prove statutory diligence to the regulators and prevent penalties and reputational damage.

Together, they create a closed-loop system where risks are ongoingly monitored, addressed, documented protecting the Company from financial crime and regulatory fallout.

10.1. INTERNAL REPORTING

Internal AMLCTF reporting consist of:

- Unusual and Complex Transactions Reports;
- Efficiency Control Reports;
- Annual AMLCTF System Activity Reports.

a) Unusual and Complex Activity Report

Unusual and Complex Activity Report is an output of CDD / Sanctions ongoing monitoring process.

The aim of CDD / Sanctions ongoing monitoring process is to determine risks related to the client and client business activity, to understand and consequently mitigate those risks.

During CDD / Sanctions ongoing monitoring process the 1^{st} or 2^{nd} level employee conducting client reviews and ongoing monitoring and screening controls is obliged to determine unusual or complex client / transaction activity.

Unusual or complex client activity refers to transactions or behaviour that deviates from the client's usual pattern that is aligned with the profile of client's business model. Identification of unusual and complex client activity is important because it represent input for STR reporting.

The Company identifies unusual / complex and potentially suspicious client activity by taking in consideration specific set of indicators specified by FINTRAC disposable on FINTRAC website.[9]

Unusual and Complex Activity Report serves as a tool for documentation of unusual or complex client activity and input to MLRO for the potential STR reporting.

Employees of the 1st and 2nd line AMLCTF form are obliged to fill out Unusual and Complex Activity Report whenever they detect unusual or complex client behaviour during CDD / Sanctions monitoring process.

Form for submission of Unusual and Complex Activity Report is enclosed via *Annex 2 - Unusual and Complex Activity Report* to this AMLCTF Policy.

b) Efficiency Control Report

MLRO reports efficiency control outcomes to the Management via Efficiency Control Report in a concise, data-driven and action-oriented manner.

The report should include:

- Executive summary with brief overview of AML/CTF program performance, major risks, key achievements and highlighting critical issues requiring management attention;
- Controlled area Key Performance Indicators;
- Control testing and sample analysis – applied methodology, sample size, findings, remediation proposals;
- Risk and compliance updates -changes in regulatory requirements and alignment status, emerging typologies;
- Recommendations for next steps.

c) Annual AMLCTF System Activity Report

MLRO provides ongoing guidance to Management on necessary measures to ensure full compliance with applicable laws, regulations, and industry standards.

This includes impact of regulatory changes on the Company's operations and its financial crime monitoring framework.

Within the annual report MLRO highlights critical areas for Management's attention including identified gaps, remediation progress and resource allocation.

[9] FINTRAC: MSB INDICATORS

The annual report for the previous year until the end of March of current year must and include at a minimum, the following sections:

- Executive summary with key outcomes of Company-wide MLTF risk assessment;
- Methodology updates with description of any changes to client risk assessment process and their alignment with the Company overall risk profile;
- Client risk segmentation with breakdown of clients by risk category, noting overdue CDD reviews;
- Transaction monitoring statistics: Unusual and Complex Activity Reports, STRs, business relationship terminated due to unmitigated MLTF risks, information requests received from regulatory and law enforcement authorities;
- Evaluation of AMLCTF organisation structure and human and technical resources;
- Summary of new/updated policies, identified deficiencies and corrective actions;
- Overview of monitoring measures and system effectiveness;
- Audit findings;
- Regulatory engagement in the terms of details of supervisory communications, violations, sanctions and corrective measures.

10.2. STATUTORY REPORTING

In accordance with applicable AMLCTF Legislation of Canada and in the scope of MSB activities and business model the Company is obliged to submit following reports to FINTRAC:

- Suspicious Transaction Reports;
- Listed Person or Entity Property Reports;
- Large Virtual Currency Transaction Reports;
- Electronic Fund Transfers Reports.

MSBs in Canada are as well required to report Large Cash transaction Reports to FINTRAC, however processing cash is not within the Company’s business model this AMLCTF Policy does not include them within applicable statutory reports.

a) Suspicious Transaction Report

The Company submits STR report to FINTRAC at instances when MLRO determines *reasonable grounds to suspect* that the transaction, or attempted transaction is related to MLTF offence.

Reaching reasonable grounds to suspect the Company's services are used for commission of MLTF offence implies that MLRO has considered the facts (date, time, location, amount, business lines, financial history etc.) the context (client risk assessment CDD or other illustrative client details), MLTF indicators and sanctions evasion characteristic related to monitored transaction and determined that there is a possibility of MLTF offence.

STR reporting is not related with any monetary threshold.

In the terms of STR reporting schedule, STR should be reported *as soon as practicable* after completing measures which enable MLRO to establish reasonable grounds for MLTF suspicion and not later than 30 days after establishing MLTF suspicion.

Results of investigation that takes place during client monitoring process and information submitted via Unusual and Complex Transaction Report the Company regards as prerequisites for establishment of MLTF suspicion.

STRs can be submitted to FINTRAC via FINTRAC Web Reporting System (FWR) that is geared towards entities with lower reporting volumes, FINTRAC API report submission which is secure system-to-system transfer of report information, or in paper form.

Considering the size, scope and reporting volumes the Company will submit STR reports via FINTRAC Web Reporting system.

Alternatively, in case of a system failure the Company will submit STR using Paper reporting form[10] either by fax: 1-866-266-2346, or by post directed on address: Financial Transactions and Reports Analysis Centre of Canada, Section A, 234 Laurier Avenue West, 24th floor, Ottawa, ON K1P 1H7, Canada.

10 https://fintrac-canafe.canada.ca/reporting-declaration/form/STR-eng.pdf

b) Listed Person or Entity Property Report

Upon detection, MLRO is required to immediately report property of a client determined as a listed persons.

For the purposes of this report and in the scope of the provision of MSB services, property implies monetary instruments, virtual currency, prepaid payment product and prepaid payment account.

Listed person a an individual or terrorist group listed on United Nations Security Council Consolidated List and /or Consolidated Canadian Autonomous Sanctions List.

The input for submission of this reported is derived from outcomes of sanction screening controls.

The report can be submitted to FINTRAC in Paper form[11] only either by fax: 1-866-266-2346, or by post directed on address: Financial Transactions and Reports Analysis Centre of Canada, Section A, 234 Laurier Avenue West, 24th floor, Ottawa, ON K1P 1H7, Canada.

c) Large Virtual Currency Report

MLRO is required to report all transactions in virtual currencies exceeding countervalue CAD 10.000,00, either in single amount or conducted through series of client connected transaction processed within 24 hours.

Reporting deadline is 5 business days from the transaction processing.

Exemption from reporting obligation can be applied:

- When large virtual currency transaction is conducted between two regulated entities;
- When large virtual currency transaction is conducted between persons that are not residents of Canada, when transaction does not involve CAD or funds linked to Canada, when transaction is conducted through financial entity not registered in Canada.

Considering the size, scope and reporting volumes the Company will submit Large Virtual Currency Reports reports via FINTRAC Web Reporting system.

Alternatively, in case of a system failure, the Company will submit Large Virtual Currency Reports using Paper reporting[12] form either by fax: 1-866-266-2346, or by post directed on address: Financial Transactions and Reports Analysis Centre of Canada, Section A, 234 Laurier Avenue West, 24th floor, Ottawa, ON K1P 1H7, Canada.

[11] https://fintrac-canafe.canada.ca/reporting-declaration/form/lpepr-eng.pdf

[12] https://fintrac-canafe.canada.ca/reporting-declaration/form/LVCTR-eng.pdf

d) Electronic Fund Transfer Report

The Company must report every international electronic fund transfer exceeding CAD 10.000,00 (or equivalent in foreign currency) either in single amount or conducted through series of connected client connected transaction processed within 24 hours.

This requirement pertains to all outgoing transfers send from Canada to another country or all incoming transfers received in Canada from abroad.

Exemptions from reporting constitute:

- Transfers between two regulated entities;
- Domestic transfers within Canada;
- No Canadian nexus: neither sender or recipient is Canadian resident, CAD is not involved and neither Canadian financial intermediary.

Report is submitted by MLRO, the latest 5 business days from transaction processing.

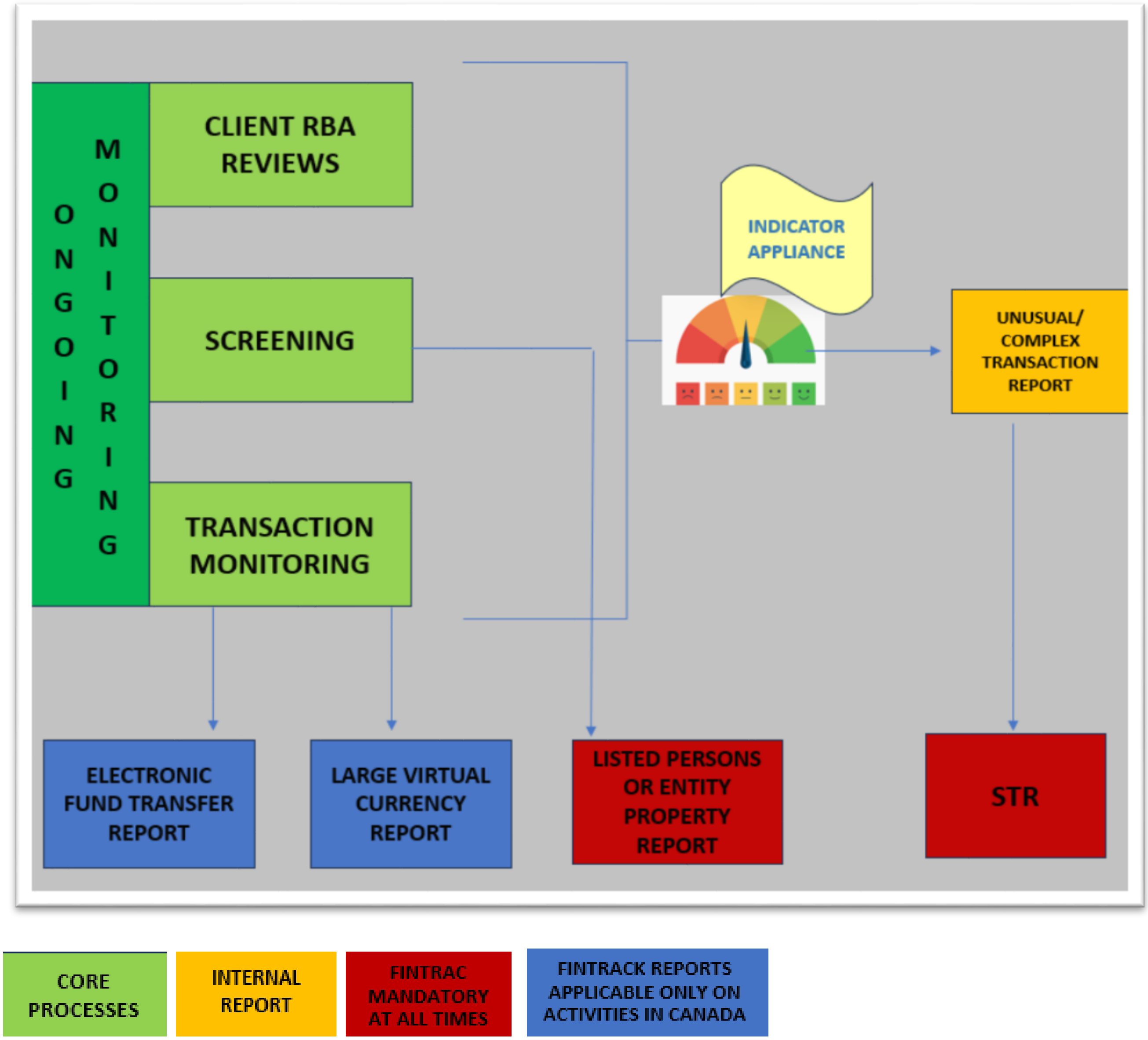
Considering the size, scope and reporting volumes the Company will submit Electronic Fund Transfer Reports reports via FINTRAC Web Reporting system.

Alternatively, in case of a system failure, the Company will submit Electronic Fund Transfer Reports using Paper reporting forms[13] [14]either by fax: 1-866-266-2346, or by post directed on address: Financial Transactions and Reports Analysis Centre of Canada, Section A, 234 Laurier Avenue West, 24th floor, Ottawa, ON K1P 1H7, Canada.

[13] https://fintrac-canafe.canada.ca/reporting-declaration/form/EFTR-Initiation-form-eng.pdf

[14] https://fintrac-canafe.canada.ca/reporting-declaration/form/EFTR-finalreceipt-eng.pdf

10.3. OPERATIONS REPORTING PROCESS FLOWCHART



11. TRAINING AND AWARENESS

In rapidly evolving landscape of financial technology, robust training and awareness programs are not merely regulatory obligations, they are the bedrock of operational excellence, risk mitigation and sustained innovation.

As Company operates within the dynamic fintech sector, navigating complex regulatory framework and ever-shifting customer expectations, fostering a culture of continuous learning is not just advantageous, but indispensable.

Therefore, the Company establishes a structured training system designed to equip employees with the expertise to identify, assess, and mitigate MLTF risks.

MLRO is responsible for delivering systematic training on:

- MLTF risks specific to the Company's operations;
- Emerging MLTF methods, trends and typologies;
- The Company's risk assessment methodology and mitigation strategies.

Training is categorized into internal and external programs, each tailored to organizational needs.

a) External training

External training serves as a critical conduit for key AMLCTF personnel to remain conversant of evolving regulatory landscapes and emerging MLTF typologies.

Typically covering MLRO, with participation extended to AMLCTF front line personnel upon budgetary provisions, these sessions are curated to address contemporary challenges.

MLRO presents proposals for external training sessions to the Management for formal approval.

TO ensure ongoing professional development MLRO is required to complete at least one external training annually, with all participation diligently documented for compliance purposes.

b) Internal training

Complementing these external engagements, the Company's Internal Training program is designed to cultivate organization-wide AML/CFT awareness, calibrated to the specific risk exposures of various functions.

MLRO prepares an annual training plan, adopted by the Management prior to year-end, which incorporates a spectrum of initiatives.

These include risk-tailored content aligned with the Company's business activities, interactive group workshops to reinforce collaborative learning, specialized onboarding sessions for new employees, and comprehensive awareness programs for all employees involved in payment transactions, spanning operational, control, and managerial roles.

Recognizing the varied risk exposure across teams, training content is thoughtfully customized to ensure relevance and impact. Post-training evaluations, including assessments and testing mechanisms, are employed to gauge effectiveness and identify opportunities for enhancement.

12. RECORD KEEPING

In accordance with Canada's AMLCTF legislation, the Company must maintain detailed records to support compliance efforts and facilitate regulatory oversight.

These requirements form an essential foundation for transparency and accountability within our financial operations, encompassing not only transactional data but also comprehensive documentation of training programs, policies, procedures, and risk assessments.

The Company is obligated to retain thorough documentation related to client identification, business relationships, and financial transactions. This includes preserving records that verify customer identity, such as government-issued identification documents or corporate records for entity clients, along with details of the methods used for verification. For ongoing business relationships, documentation must demonstrate the purpose and intended nature of the account or service arrangement.

Transaction records must be carefully maintained, capturing all relevant details for transfers of $1,000 or more, including the date, amount, currency type, parties involved, and nature of the transaction. Particular attention must be given to large virtual currency transactions, where wallet addresses, and transaction hashes should be preserved alongside traditional payment details.

The Company must maintain complete records of all AML/CTF training programs, including training materials, attendance records, assessment results, and certifications. These records should reflect both internal sessions and external training participation, particularly for compliance personnel and senior management, demonstrating our commitment to ongoing compliance education.

The foundation of our compliance program lies in its written policies and procedures.

The Company must maintain current versions of all AML/CTF documentation, including customer due diligence protocols, suspicious transaction reporting procedures, and risk assessment methodologies. These documents must show evidence of regular review and approval by the Management, with version control tracking all updates made in response to regulatory changes or operational developments.

Periodic risk assessments and their supporting documentation must also be preserved, demonstrating how the Company identifies, evaluates, and mitigates money laundering and terrorist financing risks across our products, services, and geographic operations. These assessments must be reviewed at least annually or when material changes occur in our business environment.

All records, including client information, transaction data, training documentation, policies, procedures, and risk assessments must be kept in a manner that permits their timely retrieval and review.

The standard retention period extends to **five years** from the date of transaction, the termination of a business relationship, or the last relevant action, whichever occurs latest. These records must be made available to regulators or other authorized entities upon request.

The integrity and security of these records are of critical importance.

The Company must implement appropriate safeguards to protect sensitive information from unauthorized access, alteration, or destruction while ensuring complete preservation of the original data. This comprehensive approach to record-keeping not only fulfills our regulatory obligations but strengthens our ability to monitor activity, identify potential risks, and demonstrate our culture of compliance with Canada's financial integrity framework.

13. FINAL PROVISIONS

All amendments and supplements to this Policy shall be adopted by the Company's Management upon the proposal of MLRO.

If any provisions of this Policy are superseded by new regulations, such new regulations shall apply until such time as this Policy is formally amended and updated accordingly.

14. ANNEXES

Annex 1 – Unusual and Complex Transaction Report